



INTERNET OF THINGS APPLICATIONS AND TECHNOLOGY

Edited by

Faheem Syeed Masoodi, Alwi M. Bamhdi,
Ankush Manocha, Tawseef Ahmed Teli,
Zubair Sayeed Masoodi, and Faheem Ahmad Reegu

An **Auerbach** Book



CRC Press
Taylor & Francis Group

Internet of Things Applications and Technology

The book provides a comprehensive examination of the integration of IoT technology into various industries and its impact on daily life, with a focus on the most recent advancements in the field. The technical aspects of IoT are thoroughly discussed, including the implementation of cutting-edge sensors, data communication protocols, and network topologies. The book also covers the latest advancements in areas such as edge computing, 5G networks, and AI-powered IoT devices. Emphasis is placed on the examination of IoT in real-world applications, including healthcare, agriculture, transportation, and home automation. Other highlights of the book include:

- IoT-based systems for monitoring air and water quality
- Wearable devices for continuous monitoring of vital signs and other health metrics
- IoT-based systems for monitoring and optimizing crop growth and yields
- Connected vehicles for improved safety, efficiency, and traffic management
- Monitoring of goods and resources in transit to optimize delivery times

With case studies and real-world examples, readers gain a comprehensive understanding of how IoT is revolutionizing various industries and enhancing daily life. This book is a comprehensive guide to the exciting world of IoT and its practical application.

Dr. Faheem Syeed Masoodi is an assistant professor in the Department of Computer Science, University of Kashmir, Jammu and Kashmir, India. Earlier, he held that position at the College of Computer Science, University of Jizan, Saudi Arabia, for his doctorate programme by the UGC, New Delhi.

Dr. Alwi M. Bamhdi is an associate professor in the Department of Computer Sciences, Umm Al-Qura University, Saudi Arabia.

Dr. Ankush Manocha is an assistant professor at the School of Computer Applications, Lovely Professional University (LPU), Phagwara, Punjab, India.

Dr. Tawseef Ahmed Teli is an assistant professor in the Department of Computer Science, Government Degree College, Anantnag, Jammu and Kashmir, India.

Dr. Zubair Sayeed Masoodi is an assistant professor at the School of Computer Applications, Government Degree College for Women, Sopore, Jammu and Kashmir, India.

Dr. Faheem Ahmad Reegu is a senior lecturer in the Department of Computer and Network Engineering at Jazan University, Saudi Arabia.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Internet of Things Applications and Technology

Edited by

Faheem Syeed Masoodi

Alwi M. Bamhdi

Ankush Manocha

Tawseef Ahmed Teli

Zubair Sayeed Masoodi

Faheem Ahmad Reegu



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

AN AUERBACH BOOK

Cover: www.shutterstock.com

First edition published 2025

2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press

4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

© 2025 Taylor & Francis Group, LLC

Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers. For permission to photocopy or use material electronically from this work, access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact mpkbookspermissions@tandf.co.uk

Trademark notice: Product or corporate names may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe.

ISBN: 978-1-032-59395-1 (hbk)

ISBN: 978-1-032-60268-4 (pbk)

ISBN: 978-1-003-45840-1 (ebk)

DOI: 10.1201/9781003458401

Typeset in Garamond

by MPS Limited, Dehradun

Contents

Contributors	xv
---------------------------	-----------

1	An Overview of Internet of Things (IoT)	1
	MANAS RANJAN MOHAPATRA AND SAISMITA MOHAPATRA	
1.1	Introduction	1
1.2	IoT History	1
1.3	Objectives of IoT	3
1.4	IoT Software and Hardware	3
1.4.1	IoT Software	3
1.4.2	IoT Hardware	5
1.5	Applications of IoT	7
1.6	IoT Architecture	8
1.6.1	Three-Layer and Five-Layer Architecture	8
1.6.2	Cloud-Based Architecture	10
1.6.3	Fog-Based Structure	11
1.6.4	SoA-Based Architecture	11
1.7	Privacy vs Security in IoT	12
1.8	Conclusion	13
2	IoT Architecture, Applications, Security and Privacy Issues	16
	A. HARINI, MANJULA DEVARAKONDA VENKATA,	
	CHANDRA SEKHAR KOPPIREDDY, AND G. VIJAYA KUMAR	
2.1	Introduction	16
2.2	IoT Architecture	17
2.3	Security and Privacy in IoT	21
2.4	Security Issues	21
2.5	IoT Applications and Need for Security	25
2.6	Security and Privacy Challenges in IoT	27
2.7	Conclusion	28

3 Current Trends in IoT Data Management: An Investigative Study 30
KATTU JAHNAVI, ADDANKI SNEHITHA NAGA SAI LALITHA, AND MANAS KUMAR YOGI

3.1 Introduction 30

3.1.1 Components of IoT 31

3.1.2 Applications of IoT 31

3.1.3 Data Management 31

3.1.4 Components of Data Management 32

3.1.5 Applications 32

3.1.6 IoT Data Collection and Storage 33

3.1.7 Data Collection 33

3.1.8 Data Storage 33

3.2 Stream Processing in IoT Data Management 34

3.3 Security and Privacy in IoT Data Management 35

3.3.1 Security in IoT Data Management 35

3.3.2 Types of IoT Device Security 35

3.3.3 Privacy in IoT Data Management 37

3.4 Data Visualization and Reporting 37

3.4.1 Data Visualization 37

3.4.2 Data Reporting 38

3.5 IoT Data Monetization and Business Models 39

3.5.1 Monetization and Business Models in IoT Data Management 39

3.6 Future Trends and Case Studies in IoT Data Management 39

3.6.1 Future Trends in IoT Data Management 39

3.7 Case Studies in IoT Data Management 40

3.7.1 Precision Agriculture and Crop Management IoT Data Management 40

3.8 Conclusion 40

4 A Study on the Impact of Internet of Things Development and Future Spectrum 43
HE YIGANG, FARHAN ALI, CHENGWEIDING, AND AIT MOUHA RADOUAN

4.1 Introduction 43

4.1.1 Future-Specific Applications and Examples of IoT 48

4.2 IoT Standards and Framework 48

4.2.1 6LoWPAN 49

4.2.2 Zigbee 49

4.2.3 OneM2M 50

4.3 IoT Architecture 50

4.3.1 Perception Layer 51

4.3.2	Transport Layer.....	51
4.3.3	4G LTE/5G Wi-Fi Bluetooth LPWAN	52
4.3.4	Processing Layer	52
4.3.5	Business Layer	52
4.4	Future Advancements.....	53
4.5	Conclusion.....	56
5	Revolutionizing Retail: IoT Applications for Enhanced Customer Experience	60
	USHMITA GUPTA, PRITESH SOMANI, NITESH BEHARE, RASHMI MAHAJAN, MEENAKSHI SINGH, AND C.A. VISHWANATHAN IYER	
5.1	Introduction	60
5.2	Introduction to the Retail Industry.....	61
5.3	Overview of IoT	62
5.4	Overview of the Importance of Customer Experience in the Retail Industry.....	63
5.5	Role of IoT in Transforming and Personalizing Customer Experiences	63
5.6	Understanding Customer Expectations in the Digital Age.....	64
5.7	The Demand for Personalized and Seamless Shopping Experiences	65
5.8	Understanding How Personalization Pays Off.....	66
5.9	IoT-enabled Personalization and Customization	68
5.10	Leveraging IoT Data for Personalized Product Recommendations.....	68
5.11	Personalized Shopping Experience.....	70
5.12	Importance of Personalized Shopping Experience.....	70
5.13	Examples of Personalized Customer Experience	72
5.14	Smart Retail Environments	73
5.15	Smart Shelves and Digital Signage for Interactive and Engaging Displays.....	75
	5.15.1 Smart Shelves.....	75
	5.15.2 Digital Signage	75
5.16	Some of the Benefits of Smart Shelves and Digital Signage	76
5.17	Real Time Inventory Management System and Product Availability.....	76
5.18	Conclusion	78

6	Healthier Horizons: Exploring IoT's Impact on Education and Well-Being	81
	MOHAMMAD AMIN DAR, INSHA RASOOL, AND FAHEEM SYEED MASOODI	
6.1	Introduction	81
6.2	Literature Review.....	82
6.3	The Use of IoT Devices in Early Childhood Education	83
6.4	The Use of IoT Devices in Higher Education.....	84
6.4.1	Smart Classrooms	85
6.4.2	Wearable Devices	85
6.4.3	Smart Campus.....	85
6.5	The Impact of IoT Technology on Education in 2023	86
6.5.1	Increased Adoption of IoT Devices in Education.....	86
6.5.2	Enhanced Personalization of Learning Experiences	86
6.5.3	Improved Data-Driven Decision Making	87
6.5.4	Increased Collaboration and Communication	87
6.5.5	Enhanced Innovation and Creativity	87
6.6	The Role of IoT in Education	88
6.6.1	Students.....	88
6.6.2	Educators.....	88
6.6.3	Policymakers.....	89
6.6.4	Researchers	89
6.7	Impact on Academic Outcomes	90
6.8	Personalized Learning Experiences.....	90
6.9	Real-Time Data Analysis.....	91
6.10	Conclusion	92
7	Integration of Unmanned Aerial Vehicles (UAVs) and IoT for Crop Monitoring and Spraying	95
	TARUN KUMAR VASHISHTH, VIKAS SHARMA, KEWAL KRISHAN SHARMA, SACHIN CHAUDHARY, BHUPENDRA KUMAR, AND RAJNEESH PANWAR	
7.1	Introduction	95
7.1.1	Overview of the Integration of UAVs and IoT in Agriculture	96
7.1.2	Importance of Crop Monitoring and Spraying in Modern Agriculture	97
7.1.3	Limitations and Usefulness of Using UAVs and IoT for Crop Management	98
7.2	Literature Review.....	100
7.3	Unmanned Aerial Vehicles (UAVs) in Agriculture.....	101
7.3.1	Crop Monitoring and Assessment	102
7.3.2	Precision Agriculture	102

7.3.3	Crop Mapping and Inventory.....	102
7.3.4	Irrigation Management.....	102
7.3.5	Crop Spraying and Pest Management.....	102
7.3.6	Environmental Monitoring.....	103
7.3.7	Risk Assessment and Insurance.....	103
7.3.8	Safety and Efficiency.....	103
7.4	Internet of Things (IoT) in Agriculture.....	104
7.4.1	Precision Agriculture.....	104
7.4.2	Smart Irrigation.....	104
7.4.3	Livestock Monitoring.....	104
7.4.4	Crop Health Monitoring.....	104
7.4.5	Weather Monitoring and Forecasting.....	105
7.5	Crop Monitoring with UAVs and IoT.....	105
7.5.1	Aerial Imaging and Sensing.....	105
7.5.2	Real-Time Monitoring.....	105
7.5.3	Spatial and Temporal Crop Variability.....	105
7.5.4	Early Detection of Crop Issues.....	106
7.5.5	Integration with Other Agricultural Technologies.....	106
7.6	Crop Spraying with UAVs and IoT.....	106
7.6.1	Precision Application.....	106
7.6.2	Site-Specific Treatment.....	107
7.6.3	Reduced Environmental Impact.....	107
7.6.4	Safety and Accessibility.....	107
7.6.5	Scalability and Adaptability.....	107
7.7	Communication and Data Management in UAV-IoT Integration.....	108
7.7.1	Wireless Connectivity.....	108
7.7.2	Sensor Data Acquisition.....	108
7.7.3	Cloud-Based Data Storage.....	108
7.7.4	Instantaneous Information.....	108
7.7.5	Integration with Visualization Tools.....	109
7.8	Systems That Support Decisions Using Studying Data.....	109
7.8.1	Data Preprocessing.....	109
7.8.2	Parametric Analytics.....	109
7.8.3	Prediction Analytics.....	109
7.8.4	Prescriptive Analytics.....	110
7.8.5	Decision Support Systems.....	110
7.8.6	Optimization and Resource Allocation.....	110
7.8.7	Real-Time Monitoring and Alerts.....	110
7.8.8	Continuous Improvement and Adaptation.....	110
7.9	Case Studies.....	111

7.9.1	Case Study 1	111
7.9.2	Case Study 2	111
7.9.3	Case Study 3	111
7.10	Challenges and Future Directions	112
7.10.1	Regulatory and Legal Considerations for UAVs in Agriculture	112
7.10.2	Security and Privacy Concerns in UAV-IoT Systems	113
7.10.3	Emerging Technologies and Future Trends in UAV-Based Crop Monitoring and Spraying	113
7.11	Conclusion	115
7.11.1	Recap of Key Findings and Contributions	115
7.11.2	Summary of the Potential of UAVs and IoT for Irrigation and Harvest Surveillance	115
7.11.3	Future Prospects and Recommendations for Further Research and Development	115
8	Health-Tracking System through the Application of IoT	118
	KAUSHIK BANERJEE AND SUDIPTA ADHIKARY	
8.1	Introduction	118
8.2	Literature Survey	119
8.3	Proposed Work	119
8.3.1	Smart Watch	120
8.4	Smartphone	122
8.5	Thing Speak	123
8.6	IFTTT	123
8.7	Results	124
8.8	Conclusion	124
9	IoT-Enabled Financial Inclusion: Challenges, Opportunities, and Policy Implications	126
	KHURSHID ALI GANAI, BILAL AHMAD PANDOW, AND FAHEEM SYEED MASOODI	
9.1	Introduction	126
9.2	Background and Significance of IoT-Enabled Financial Inclusion	128
9.3	Research Objectives and Scope	129
9.4	Conceptual Framework	130
9.5	Relevance to Financial Inclusion	132
9.6	Challenges of IoT-Enabled Financial Inclusion	134
9.7	Opportunities for IoT-Enabled Financial Inclusion	135
9.8	Successful Implementations of IoT-Enabled Financial Inclusion Initiatives	137

9.9	Policy Implications and Regulatory Considerations	139
9.10	Future Directions and Research Agenda	141
9.11	Conclusion	143
10	Enhancing the Security of Pregnancy Health Data Transmission through Homomorphic Encryption: An Advanced Model	146
	MOHAMMAD MOBARAK HOSSAIN, NASIM MAHMUD NAYAN, AND MOHAMMOD ABDUL KASHEM	
10.1	Introduction	146
10.2	Related Work	148
	10.2.1 Systematic Review	151
10.3	Methods and Materials	151
	10.3.1 Homomorphic Encryption	151
	10.3.2 Homomorphic Encryption in Data Security	161
	10.3.3 Homomorphic Encryption in Data Transmission	161
10.4	Our Proposed Model.....	163
10.5	Activity Diagram.....	165
10.6	Conclusion	166
11	E-Health Data Acquisition System for Detection and Prevention of Cardiac Diseases Utilizing IoT	170
	ADARSH RAVI MISHRA AND MANOJ KUMAR PANDEY	
11.1	Introduction	170
	11.1.1 Importance of IoT in Healthcare	170
11.2	Literature Review.....	171
	11.2.1 Wireless Health Supervision Apparatus.....	172
	11.2.2 Bio Signal Sensor	172
	11.2.3 Electro Cardiogram (ECG)	172
11.3	Methodology.....	172
	11.3.1 Context	173
	11.3.2 Bio Monitoring Electrodes, Sensors and Components.....	174
11.4	Hardware Requirements	175
	11.4.1 Raspberry Pi3 Model.....	175
	11.4.2 Oscillating System	175
	11.4.3 Pulse Sensor	175
	11.4.4 Micro Electro Mechanical System (MEMs).....	176
	11.4.5 ZIGBEE Technology.....	176
	11.4.6 Alternative Main Processing Devices	176
11.5	Result and Discussion	178
11.6	Conclusion and Future Scope.....	181

12	Challenges of Image Processing-Based Applications in the Analytics of Internet of Things.....	184
	MOHAMMAD IDREES BHAT, ARIF MOHAMMAD LATTOO, AND SHUBHALAXMI JOSHI	
12.1	Introduction	184
12.2	Challenges of Image Processing-Based Applications in Internet of Things (IoT) Analytic	186
12.2.1	Heterogeneity.....	186
12.2.2	Varying Quality	187
12.2.3	Real-Time Nature.....	187
12.2.4	Time and Location	187
12.2.5	Privacy and Security	187
12.2.6	Bias	188
12.3	Conclusion	188
13	Internet of Things for Smart Agricultural Practices	190
	WASSWA SHAFIK, ALI TUFAIL, ROSYZIE ANNA AWG HAJI MOHD APONG, AND LIYANAGE CHANDRATILAK DE SILVA	
13.1	Introduction	190
13.1.1	The Contribution of the Chapter	193
13.1.2	The Chapter Organization.....	194
13.2	IoT Sensors and Devices for Smart Agriculture.....	194
13.2.1	Soil Monitoring.....	195
13.2.2	Crop Monitoring	196
13.2.3	Livestock Monitoring	198
13.3	Data Collection and Data Analysis	199
13.3.1	Data-Gathering Techniques	199
13.3.2	Data Analytics and Processing	201
13.3.3	Predictive Analytics and Decision Support Systems...	202
13.4	Automation and Control Systems	202
13.4.1	Smart Irrigation.....	202
13.4.2	Precision Farming.....	203
13.4.3	Livestock Management	204
13.5	Connectivity and Communication.....	205
13.5.1	Wireless Communication Technologies.....	205
13.5.2	Data Security and Privacy Considerations	207
13.6	Selected Case Studies	208
13.6.1	Smart Irrigation System with IoT Sensors	208
13.6.2	Livestock Monitoring with Wearable IoT Devices...	208
13.6.3	Crop Monitoring and Pest Management with IoT and AI.....	208
13.6.4	Smart Greenhouses with IoT Automation	209

13.7	Future Trends and Challenges	210
13.7.1	Integration with Emerging Technologies	210
13.7.2	Edge Computing and Edge Analytics.....	210
13.7.3	Sustainable and Regenerative Practices.....	211
13.7.4	Data Interoperability and Standardization	211
13.7.5	Data Privacy and Security	211
13.7.6	Digital Divide and Accessibility.....	211
13.8	Lessons Learnt and Conclusion	211
14	Smart IoT-Based Air Quality Monitoring System	218
	S. DEVI MAHALAKSHMI, S. KARKUZHALI,	
	AND G. SHENBAGALAKSHMI	
14.1	Introduction	218
14.2	Literature Survey	219
14.3	Methodology.....	219
14.3.1	Input.....	220
14.3.2	Smart Citizen Kit.....	220
14.3.3	Smart Citizen Website	221
14.3.4	Curve Fitting.....	223
14.3.5	Prediction of Gas	223
14.4	Results and Discussion	223
14.4.1	Sensing the Air Quality	223
14.4.2	Posting Data to the Website.....	224
14.4.3	Uploading and Downloading Data	228
14.4.4	Prediction Using Linear Regression	228
14.4.5	Importing the Libraries and Read Independent Variable.....	228
14.4.6	Visualizing and Fitting Linear Regression	229
14.4.7	Predicting the Gas Level	229
14.4.8	Input	229
14.4.9	Sending Data to Website.....	230
14.4.10	Prediction of Gas Using Linear Regression	230
14.5	Conclusion	231
15	Smart Shoes for Vision Disabled	234
	JANHVI MISHRA AND DIVYANSHU TIWARI	
15.1	Introduction	234
15.2	Smart Devices and Their Use in Our Project	235
15.2.1	Devices Required	236
15.2.2	Arduino (UNO, NANO) Arduino Uno.....	236
15.2.3	General Functions of the Pins Used	237
15.2.4	Special Pin Functions	238
15.2.5	Specialized Functions of the Pins	239

15.2.6	Arduino Nano.....	239
15.2.7	Ultrasonic Sensor.....	239
15.2.8	Ultrasonic “Waves”	240
15.2.9	To Interface an Ultrasonic Sensor	241
15.2.10	Fire Detection Sensor.....	242
15.2.11	Vibration Sensor.....	243
15.2.12	Tracker	244
15.2.13	Battery	244
15.3	About the Model.....	244
15.4	Results and Analysis	246
15.5	Conclusion	247
Index		248

Contributors

Sudipta Adhikary

School of Law
Brainware University
Barasat, Kolkata, West Bengal, India

Shikha Agnihotri

Institute of Management Studies
Lal Quan, Ghaziabad, Uttar Pradesh,
India

Farhan Ali

School of Electrical Engineering and
Automation
Hefei University of Technology, Hefei
China

Rosyzie Anna Awg Haji Mohd Apong

School of Digital Science
Universiti Brunei Darussalam, Bandar
Seri Begawan
Brunei Darussalam

A. Arulmurugan

Department of Computing
Technologies
SRM Institute of Science and
Technology, Chennai
Tamil Nadu, India

G. Balamurugan

Department of Computing
Technologies
SRM Institute of Science and
Technology, Chennai
Tamil Nadu, India

Kaushik Banerjee

School of Law
Brainware University
Barasati, Kolkata, West Bengal, India

Nitesh Behare

Balaji Institute of International
Business
Sri Balaji University
Pune, Maharashtra, India

Mohammad Idrees Bhat

School of Computer Science
MIT-World Peace University
Pune, Maharashtra, India

Sachin Chaudhary

School of Computer Science and
Application
IIMT University
Meerut, Uttar Pradesh, India

Mohammad Amin Dar

Department of Education
University of Kashmir
Srinagar, Jammu and Kashmir, India

Liyanage Chandratilak Desilva

School of Digital Science
Universiti Brunei Darussalam
Bandar Seri Begawan, Brunei Darussalam

Cheng Wei Ding

School of Electrical Engineering and
Automation
Hefei University of Technology
Hefei, China

Khurshid Ali Ganai

Higher College of Technology
Abu Dhabi, Dubai, UAE

Ushmita Gupta

Balaji Institute of International
Business
Sri Balaji University
Pune, Maharashtra, India

A. Harini

Pragati Engineering College
Surampalem, Andhra Pradesh, India

Mohammad Mobarak Hossain

Department of Computer Science and
Engineering
Dhaka University of Engineering and
Technology (DUET)
Dhaka, Bangladesh

C.A. Vishwanathan Iyer

Assistant Professor
Balaji Institute of International
Business
Sri Balaji University
Pune, Maharashtra, India

Kattu Jahnavi

CSE Department, Pragati Engineering
College (A)
Surampalem, Andhra Pradesh, India

Shubhalaxmi Joshi

School of Computer Science
MIT-World Peace University
Pune, Maharashtra, India

S. Karkuzhali

Department of Computer Science and
Engineering
Mepco Schlenk Engineering College
Sivakasi, Tamil Nadu, India

Mohammad Abdul Kashem

Department of Computer Science and
Engineering
Dhaka University of Engineering and
Technology (DUET)
Dhaka, Bangladesh

R. Kaviarasan

Department of Computer Science and
Engineering
Rajeev Gandhi Memorial College of
Engineering and Technology
Nandyal, Andhra Pradesh, India

Chandra Sekhar Koppireddy

Pragati Engineering College
Surampalem, Andhra Pradesh, India

Bhupendra Kumar

School of Computer Science and
Application
IIMT University
Meerut, Uttar Pradesh, India

Addanki Snehitha Naga Sai Lalitha
CSE Department, Pragati Engineering
College (A)
Surampalem, Andhra Pradesh, India

Arif Mohammad Lattoo
Sonata Software Limited
Bangalore, Karnataka, India

Rashmi Mahajan
Balaji Institute of International Business
Sri Balaji University
Pune, Maharashtra, India

S. Devi mahalakshmi
Department of Computer Science and
Engineering
Mepco Schlenk Engineering College
Sivakasi, Tamil Nadu, India

Shivani Malhan
Chitkara Business School
Chitkara University
Rajpura, Punjab, India

Faheem Syeed Masoodi
Department of Computer Science
University of Kashmir
Srinagar, Jammu and Kashmir, India

Rekha Mewafarosh
Shri Ram Institute of Management and
Technology
Kashipur, Uttarakhand, India

Adarsh Ravi Mishra
Department of CS & IT
Dr. C.V. Raman University
Bilaspur, Chhattisgarh, India

Janhvi Mishra
Christ University
Pratapgarh, Uttar Pradesh, India

Manas Ranjan Mohapatra
Department of Computer Science
Banki College (Autonomous)
Cuttack, Odisha, India

Saismita Mohapatra
Department of Computer Science
Banki College (Autonomous)
Cuttack, Odisha, India

Nasim Mahmud Nayan
Department of Computer Science and
Engineering
University of Information Technology
and Sciences (UITS)
Dhaka, Bangladesh

Manoj Kumar Pandey
Department of CS
Pranveer Singh Institute of Technology
Kanpur, Uttar Pradesh, India
and
Department of CSE
Chandigarh University
Mohali, Punjab, India

Bilal Ahmad Pandow
Bahrain polytechnic
Isa Town, Bahrain

Rajneesh Panwar
School of Computer Science and
Application
IIIT University
Meerut, Uttar Pradesh, India

Ait Mouha Radouan
School of Electrical Engineering and
Automation
Hefei University of Technology
Hefei, China

Insha Rasool

Department of Education
University of Kashmir
Srinagar, Jammu and Kashmir, India

Wasswa Shafik

School of Digital Science
Universiti Brunei Darussalam
Bandar Seri Begawan
Brunei Darussalam
and
Dig Connectivity Research Laboratory
(DCRLab)
Kampala, Uganda

Vikas Sharma

School of Computer Science and
Application
IIMT University
Meerut, Uttar Pradesh, India

Kewal Krishan Sharma

School of Computer Science and
Application
IIMT University
Meerut, Uttar Pradesh, India

G. Shenbagalakshmi

Department of Computer Science and
Engineering
Mepco Schlenk Engineering College
Sivakasi, Tamil Nadu, India

Meenakshi Singh

Balaji Institute of International
Business
Sri Balaji University
Pune, Maharashtra, India

Pritesh Somani

Balaji Institute of International Business
Sri Balaji University
Pune, Maharashtra, India

Anita Tanwar

Chitkara Business School
Chitkara University
Rajpura, Punjab, India

Divyanshu Tiwari

Sidharth University
Gorakhpur, Uttar Pradesh, India

Ali Tufail

School of Digital Science
Universiti Brunei Darussalam
Bandar Seri Begawan
Brunei Darussalam

Tarun Kumar Vashishth

School of Computer Science and
Application
IIMT University
Meerut, Uttar Pradesh, India

Manjula Devarakonda Venkata

Pragati Engineering College
Surampalem, Andhra Pradesh, India

G. Vijayakumar

Pragati Engineering College
Surampalem, Andhra Pradesh, India

He Yigang

School of Electrical Engineering and
Automation
Wuhan University
Wuhan, China

Manas Kumar Yogi

CSE Department
Pragati Engineering College (A)
Surampalem, Andhra Pradesh, India

Chapter 1

An Overview of Internet of Things (IoT)

Manas Ranjan Mohapatra and Saismita Mohapatra

Department of Computer Science, Banki College (Autonomous), Cuttack, Odisha, India

1.1 Introduction

The term Internet of Things (IoT) given by Kevin Ashton refers to the communication of devices connected to the Internet. Generally, it is considered as a huge network of interconnected devices for the purpose of data collection and sharing. IoT is continuously attempting to expand human interdependence day to day that is by interacting, contributing and collaborating to things which gradually results in less user involvement and achieving high accuracy along with more efficiency, and technological and economic advantages.

1.2 IoT History

In 1832, during the design of the first electromagnetic telegraph, the idea of connected devices emerged. This telegraph facilitated direct communication via electric signals. But, the real history of IoT started with the Internet—a much-needed piece in the later phases of 1960s that grew rapidly in the following decades [1].

This might be a tough one to have faith in, but the Coca-Cola vending machine sited at Coca-Melon University is considered as the first-ever new connected device (1980) that added a number of micro-switches to the machine. It

applied an initial version of the Internet to check if the refrigeration device would cool the drink enough and if Coke cans were available. Such a development encouraged higher study related to this area with the expansion of interconnected machines all over world.

John Romasky (1990) was the foremost person to make the connection of a toaster to the Internet using TCP/IP. In the succeeding year, Cambridge researchers used the first webcam prototype to find out the remaining coffee quantity in the container. They set up a webcam to take photos of the container thrice in a minute and forwarded these photos to nearby computers so that all could know about coffee availability.

Being the most remarkable for IoT, Kevin Ashton (1999) invented the key term “Internet of Things”. He demonstrated IoT as a technology which integrates multiple tools for supply chain management using RFID tags while imparting presentation to Proctor and Gamble. He mainly highlighted the term “Internet” in his title to describe the viewers because the Internet was a great deal in those days. Although this view of RFID-used device connectivity is different one to the current IP-oriented IoT, Ashton’s invention had a high impact on the overall improvement in technologies.

The term “Internet of Things” was used extensively by *The Boston Globe*, *Forbes* and *The Guardian* at the beginning of the 20th century. Interest in IoT technology has been steadily growing since then and it enabled the formation of the first International IoT Conference held in Switzerland (2008). Discussion on technology areas such as sensor networks, RFID, and short-range wireless communication was held by researchers from 23 nations.

Furthermore, numerous significant innovations have fueled major progress in IoT. In 2000, an Internet-connected refrigerator was built by LG Electronics that allows its customers to carry out online shopping along with making video calls. One more major invention was a tiny robot in the shape of a rabbit (2005) that tells the most recent news updates, forecasting of weather information and stock exchange updates.

Gardner hype cycle (2011) additionally supported the IoT boom for technological looming with the public launch of an IoT-centric protocol i.e. IPv6 that operates at network layer. Thereafter, interconnected devices became widespread and frequent in people’s daily lives. Strong exertion to produce IoT sensors and devices has been made by different companies like Google, Apple, Samsung, General Motors, Cisco, etc. with a wide range of smart products, e.g. smart glass, interconnected thermostats, self-driving cars. Different sectors where IoT can be applied includes, oil and energy, healthcare, transportation, retail, farming and many other industries. With this radical change, we realized that the IoT transformation is here-and-now.

Not only virtual assistants, connected homes, Level 4 auto-driven cars and others, but IoT platforms have also occupied top places in Gardner hype cycle (2018) and no doubt will occupy its top position in productivity in the coming five to ten years (Figure 1.1).

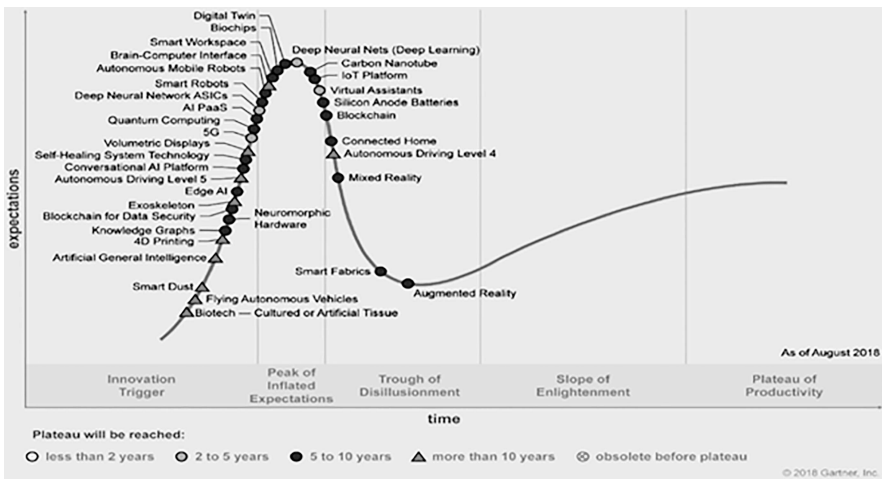


Figure 1.1 Gartner hype cycle for emerging technologies (2018).

1.3 Objectives of IoT

Communication made by the Internet expands to everything around us using IoT. The IoT is more than just M2M communications, wireless sensor networks, 2G/3G/4G, and RFIT. These are considered powerful technologies that can make use of the “Internet of Things” [2] (Figure 1.2).

Many industry, standardization and research organizations are currently involved in the development of solutions to meet specific technical requirements. This inquiry explains the current IoT state-of-the-art. More precisely:

- Provides readers with an explanation of the many perspectives on the IoT standards derived from various scientific communities.
- Reviews implementing technologies and demonstrates the key benefits of spreading these standards in everyday life.
- Suggests important research factors analysis faced by scientific communities.

The basic objective is to give reader an opportunity to understand what has already been done (protocols, methods, and proposed solutions) and what still needs to be considered, and what are the functional features of this evolution and its drawbacks and risk factors [3].

1.4 IoT Software and Hardware

1.4.1 IoT Software

Embedded system is the collection of both hardware and software. So software is as essential as hardware. As when we start to code the hardware then we need software

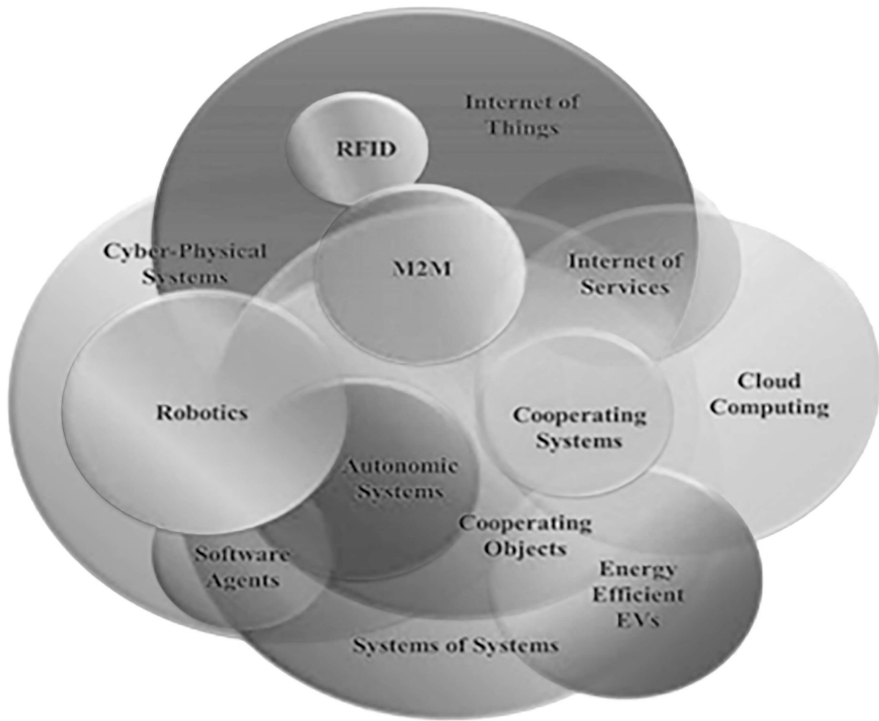


Figure 1.2 Technical convergence.

which can be used to upload the code into the hardware. After uploading the code we need an online cloud in which the data can be stored and represented in case of monitoring devices. Similarly, we need a cloud to trigger a device with respect to our signal. After all this sometime we need software to integrate different clouds and webhooks. The software support in IoT deals with the following tasks

1. Data Collection
2. Device Integration
3. Real-Time Analytics
4. Applications and Process Extension

IoT software is all about the cloud which is used to save or to show the data of all the nodes present in a system. Cloud is an online website used for collection and representation of data and it also deals with loading of program into the hardware either in form of digital data or into any other form. Some of the free available clouds are as:

1. Arduino
2. AdaFruit

3. IFTTT
4. deviceHive
5. Kaa
6. Home Assistant
7. Devicehub.net
8. SiteWhere
9. Zetta
10. Particle
11. ThinkSpeak
12. OpenRemote

All of these clouds help in integrating the hardware with a tool that can help in uploading the code in the hardware and fetching of data from hardware and to pass the data to hardware. In all of these clouds we can design the portals or dashboards as per the client requirements as well with the help of application program interface (API) we can link those dashboards to further any kind of applications. Such clouds provide a special feature of customized dashboard as with the help of one cloud we can link many devices and customize their view on cloud too.

1.4.2 IoT Hardware

To choose a proper hardware in IoT is very critical part of the whole process. Choosing the wrong hardware can also lead to failure of the product, so to choose an efficient hardware is very important. Choosing hardware or decision of choosing the same can impact many things in the system as computation power, life span, cost, etc. Whenever we are in a phase of choosing hardware we need to take all the points related of the system and have to carry out a comparison report too. As per the requirements, the hardware is used. The person responsible for the same must have that level knowledge, so that he/she can choose the most efficient and suitable hardware. As when we talk about the technology stack of the IoT, then it is like:

1. Device hardware
Choosing of hardware modules required.
2. Device software
Choosing software required in the system or to design the system.
3. Communications
Choosing communication methods between components.
4. Cloud platform
Choosing a proper cloud.
5. Cloud application
Choosing proper interfaces over cloud

With the help of above scheme it can be simply concluded that at the time of choosing hardware, the developer only has the clients he needs to have that level of experience to choose a hardware. One wrong choice of hardware can lead to a great loss of the time and resources.

When we are choosing the hardware or when any hardware choosing person does the same it flows of choosing as per four different things (base of hardware selection in any system).

1. Things

IoT deals with monitoring and controlling of devices. The unit device which needs to be controlled or which needs to be monitored is known as the things or assets. So we must take of what we need to control or monitor so that later on we can avoid the issues related to integration of the same.

2. Data Acquisition Component

As when we are monitoring or controlling devices then either we are taking physical data into digital or we are controlling physical system with the help of digital signals. In both types of system we need an intermediate which can do the conversion as per the requirement. Such intermediate devices are known as Data Acquisition devices or component.

3. Data processing component or brain of the system

To run any kind of system the main role is of brain or the unit that processes data. So brain is a component in system which performs the task of data processing in case monitoring of data and performs the task to regulate the data as per user requirements in case of controlling. The brain of any system in IoT is known as the data processor or data processing unit.

4. Communication System

The word Internet of Things itself comprises the word 'Internet'. As the Internet is a mode of communication between devices so whenever we are in a phase of choosing the hardware, we must choose a proper communication module as per the requirements.

So this is briefly the things we need to take care of before choosing the hardware in the IoT.

Some of the best IoT hardware companies are as follows:

1. Arduino
2. Particle
3. SparkFun
4. Adafruit
5. Espressif

IoT deals with four types of basic devices as follows:

1. System on Chip (SoC)
2. Programmable Logic controller (PLC)
3. Remote Terminal Unit (RTU)
4. Single Board Computer (SBC)

This all is about the awareness with respect to the system. Now the product manager needs to take care of the following things.

1. About vendor's connectivity with client.
2. Which method is going to be used for communication?
3. Cost must not be high.
4. Computation power of the brain must follow the requirements.
5. About the services provided by the vendor.
6. Place where the hardware need to be implemented.
7. Choosing proper data plans for the system.
8. Issues with the security of system.
9. Issues with privacy of the system.
10. API access power of the hardware.
11. Size of the hardware.
12. Connectivity of the hardware.
13. Integration of the hardware.

1.5 Applications of IoT

There exist a number of IoT applications spread over different types of networks which may be a small application of office automation to a larger one of industrial IoT applications. During the development of different IoT applications, we should specify the design constraints in a proper way in order to maintain the cost and efficiency [4]. Those constraints are illustrated in Figure 1.3.

Important applications of IoT can be outlined as below:

1. Smart Home
2. Smart Building
3. Smart Grid Management
4. Smart Office Management
5. Smart Healthcare Management
6. Smart Banking System
7. Smart Agricultural management
8. Smart Traffic Management

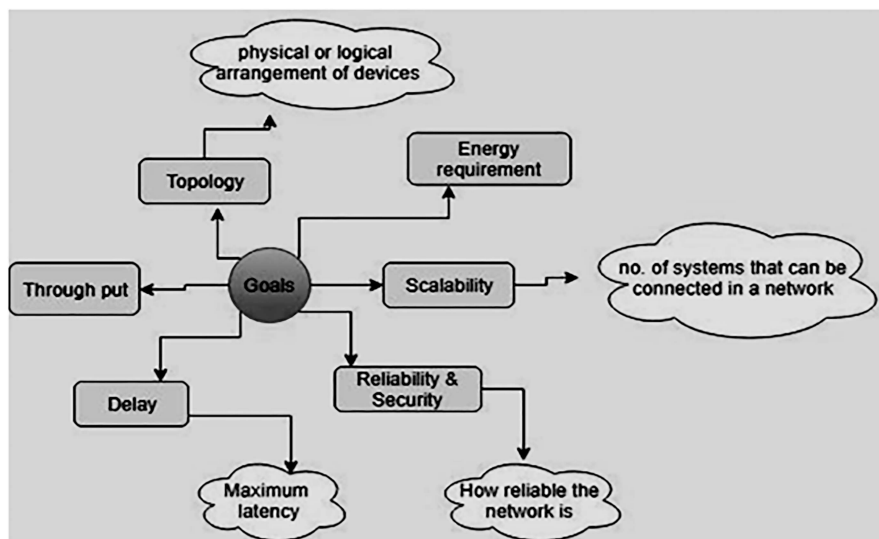


Figure 1.3 Design constraints to be specified for IoT applications.

9. Smart Retail Management
10. Smart Parking System
11. Smart Transportation System

1.6 IoT Architecture

The architecture must be flexible in nature because it must connect billions and trillions of different objects to each other. There are many recommended frameworks for IoT, but not all of them have yet been assembled to form unique reference architecture. Technological changes and research reveal several projects to develop the general architecture of the Figure 1.4 shows the three-layer architecture that is the basic form. This one came into picture in the very initial phases of this research wing consisting of three numbered layers:

IoT: From the set of existing architectures we present two structures that are frequently used by different researchers and in the industry [5].

1.6.1 Three-Layer and Five-Layer Architecture

1. Perception layer: Environmental information such as physical factors, intelligent entities are recognized, sensed and collected through sensors in this physical layer.

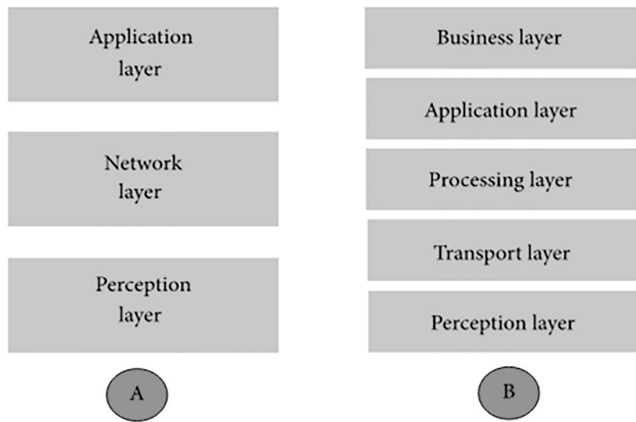


Figure 1.4 Three and five layer architecture of IoT.

2. Network layer: Connection with different intelligent entities, servers, networking devices is done, also transform and process the sensed data.
3. Application layer: Provide services based on applications that may be Smart health care, Smart home, Smart city, etc.

Basic underlying knowledge of IoT is explained by three-layer architecture, but this is inadequate for IoT research because refined aspects of the IoT sometimes needed in research. So there are a number of other layered structures. Out of this one is five-layer architecture that adds extra three layers namely [6–9] (Figure 1.4)

1. Transport layer: Transfers data between sensors and the processing layer in both ways over different network paths, for example, RFID, wireless, NFC, LAN, Bluetooth.
2. Processing layer: Stores, analyzes and processes huge data volumes coming to this layer from upper one. It handles, gives different low layer services.
3. Business layer: Maintains the complete system of IoT, which includes models of profit and business, applications and privacy of users.

Ning and Wang's [10] architecture is another one stimulated with human brain's layers of processing. Ability of thinking, feeling, remembering, reacting to the physical environment and making decision of human beings as well as intelligence motivated the design of this architecture. The three parts are:

1. Human brain: Same as data center or the unit of data management and also the processing unit.
2. Spinal cord: Same as smart gateways, inclusive of data processing nodes forming a distributed network.
3. Network of nerves: Associated with sensors along with networking elements [4].

1.6.2 Cloud-Based Architecture

Figure 1.5 demonstrates IoT's cloud-based architecture that consists primarily of four layers [11]:

1. Physical layer: contains technologies which accumulate information contained in a network's connected devices.
2. Process layer: contains technologies for storing information from connected devices in a network, additionally attempts for analyzing this information.
3. Gateway layer: contains information of networks, converts data into a suitable form for cloud services and enable the ways for end-to-end communication.
4. Cloud service: Forms an essential part of the architecture, uses algorithms of data analytics for processing of collected data. It has four parts: (Figure 1.6)
 - Broker and message queue: streamlining the incoming messages from different customers then processing those, so made the network more scalable.

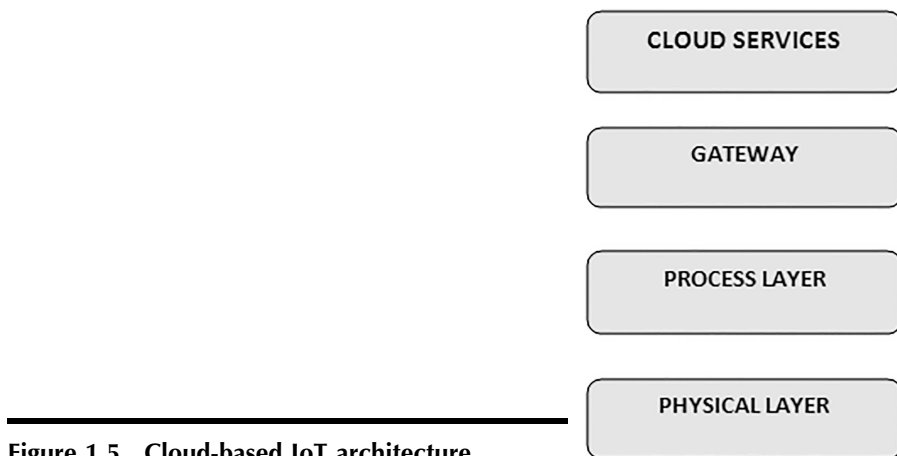


Figure 1.5 Cloud-based IoT architecture.

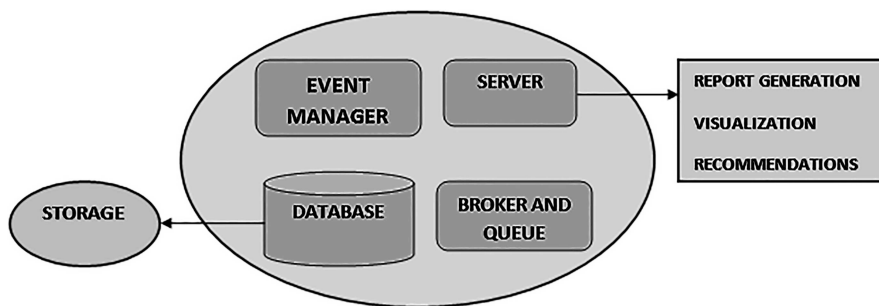


Figure 1.6 Cloud services.

- Data base: main task is to store data
- Server: displays and reports data to let the user know about data and give suggestions.
- Event managers: Carry out event-handling task. Higher priority interrupts are executed e.g. fire alarm. Under exigency condition, specific actions are triggered [12].

1.6.3 Fog-Based Structure

The cloud computing features are extended to fog computing which is the most recent technology. By monitoring the storage it provides network information of client and cloud services. It offers decentralized computing that is the computation of data, its storage and resource management are effectively distributed between the client and the cloud [11] (Figure 1.7).

There is a close resemblance between cloud computing and fog computing architecture [4] with the only disparity being the data computation is done on devices connected to the network edges. Thus, its other name is edge computing. Also, this architecture possesses higher scalability [11].

1.6.4 SoA-Based Architecture

To offer the data services in IoT and to make the architecture more flexible, here between network and application layer a service layer is included. Interfaces and protocols are employed in this model in order to connect diverse services. Software and hardware components are reused to enhance its feasibility. This architecture contains four layers. (Figure 1.8)

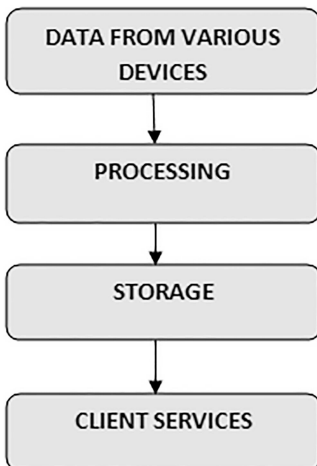


Figure 1.7 Fog-based structure.



Figure 1.8 SoA-based architecture.

1. Perception layer: This bottom layer collects sensor data.
2. Network layer: Plays a similar role as in the basic architecture such as route determination, data transmission [13].
3. Service layer: It delivers the services for application layer support and contains all facilities for identifying the desired service request, also does integration of various services to satisfy the service request needs. It has two sub-layers, service composition and service management. Service composition facilitates to communicate with the connected entities while service management manages the service requests.
4. Application layer: Same as basic architecture's application layer. All applications like smart home, smart city, etc., are supported here.

1.7 Privacy vs Security in IoT

Privacy has been treated as a part of security by a number of researchers, as the previous discussions in this context reflect [14]. There exists exceptional variance between these two despite many major overlappings along with a few intersections too [15–18]. These discrepancies are being reflected here. Privacy refers to individual persons with their specific personal/sensitive data that gives importance on no exploit of the reasons for protecting data, unauthorized data access or inappropriate use of data not as per the user. Additionally, privacy can be understood as that degree of interaction with the environment can be determined by each individual, similarly the permitted data quantity for public view can be determined too [19,20]. Security is an old term that attempts both data and device protection from outside attacks, spyware, and subversion. Commonly, hardware security is given more focus by manufacturers compared to users' privacy [21,22]. In particular, privacy invasion is possible with the collection of users' data and then applying analysis over it but in case of security, finding out information such as password of users is sufficient. Moreover, security provides data protection within trusted-parties that primarily

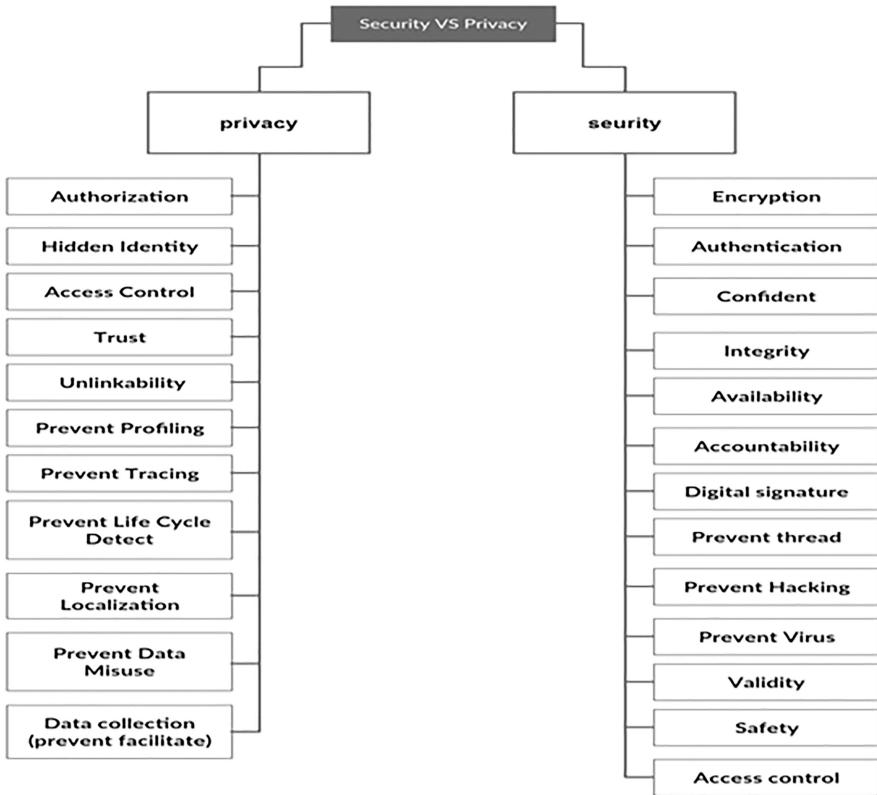


Figure 1.9 Difference between privacy and security.

involves foreign attack, but in case of privacy there are some parties which are untrusted as Service Provider (SP), which must be handled within it. This research mainly gives priority to the aspect of privacy in an IoT environment. Figure 3.1 shows the basic differences between privacy and security.

Currently, there are no such approaches that give attention to privacy-preserving of data in a device, while data preservation over links/servers having different trust levels in SP, Third Party (TP), peers and no full trust has been the main focus so far [23]. There are several examples of privacy breaks in different IoT applications i.e. smart device, social media, phone apps, LBS, smart healthcare and so on. [24, 25] (Figure 1.9).

1.8 Conclusion

A brief history of IoT and different objectives of IoT are described in this chapter. This chapter provides IoT architecture variations such as three-layer and five-layer

architecture, and cloud-based, fog-based and SOA-based architecture. It also explains the different hardware and software aspects of IoT along with its application areas. It additionally distinguishes privacy and security concept in IoT.

References

1. S. Khvoynitskaya, "The history and future of Internet of Things", <https://www.itransition.com/blog/iot-history>.
2. S. Misra et al., "Security challenges and approaches in Internet of Things", *Springer Briefs in Electrical and Computer Engineering*, 10.1007/978-3-319-44230-3_3.
3. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", *Computer Networks*, 54(15):2787–2805, 2010. 10.1016/j.comnet.2010.05.010.
4. P. Sethi, and S. R. Sarangi, "Internet of Things: Architectures, protocols, and applications", *Journal of Electrical and Computer Engineering*, 2017, 2017. 10.1155/2017/9324035
5. M. Guizani Al-Fuqaha, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications", *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, Fourthquarter 2015.
6. O. Alsaryrah Mashal, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues", *Ad Hoc Networks*, 28:68–90, 2015.
7. O. Said, and M. Masud, "Towards Internet of Things: Survey and future vision", *International Journal of Computer Networks*, 5(1):1–17, 2013.
8. M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things", In Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), 5:V5-484–V5-487, IEEE, Chengdu, China, August 2010.
9. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The Internet of Things architecture, possible applications and key challenges", In Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT '12), 257–260, December 2012.
10. H. Ning, and Z. Wang, "Future Internet of Things architecture: Like mankind neural system or social organization framework?", *IEEE Communications Letters*, 15(4):461–463, 2011.
11. H.D. Kotha, and V. Mnssvkr Gupta, "IoT application, A survey", *International Journal of Engineering & Technology*, 7(2.7):891–896, 2018.
12. A.F. da Silva, R.L. Ohta, M.N. dos Santos, and A.P.D. Binotto, "A cloud-based architecture for the Internet of things targeting industrial devices remote monitoring and control", *IFAC-PapersOnLine*, 49(30):108–113, 2016.
13. K. Kaur, "Survey on Internet of Things – Architecture, applications, and future trends", First International Conference on Secure Cyber Computing and Communication (ICSCCC)-2018. In Proceeding of IEEEExplore digital library 978-1-5386-6373-8/18.
14. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges", *Ad Hoc Network*, 10(7):1497–1516, 2012.
15. S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead", *Computer Networks*, 76:146–164, 2015.

16. J.H. Ziegeldorf, O.G. Morchon, and K. Wehrle, “Privacy in the Internet of Things: Threats and challenges”, *Security and Communication Networks*, 7(12):2728–2742, 2014.
17. J. Wang, Z. Zhang, K. Xu, Y. Yin, and P. Guo, “A research on security and privacy issues for patient related data in medical organization system”, *International Journal of Information Security*, 7(4):287–298, 2013.
18. R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed Internet of Things”, *Computer Networks*, 57(10):2266–2279, 2013.
19. J.S. Kumar and D.R. Patel, “A survey on Internet of Things: Security and privacy issues”, *International Journal of Computer Application*, 90(11), 2014.
20. H. Sundmaecker, P. Guillemin, P. Friess, and S. Woelffle, “Vision and challenges for realising the Internet of Things”, In *Cluster of European Research Projects on the Internet of Things*, European Commission, 3(3), 34–36, 2010.
21. T. Borgohain, U. Kumar, and S. Sanyal, “Survey of security and privacy issues of Internet of Things”, *International Journal of Advanced Networking and Applications*, 6:2372–2378, 2015.
22. Z. Yan, P. Zhang, and A.V. Vasilakos, “A survey on trust management for Internet of Things”, *Journal of Network and Computer Applications*, 42:120–134, 2014.
23. A. Solanas, J. Domingo-Ferrer, and A. Martínez-Ballesté, “Location privacy in location-based services: Beyond TTP-based schemes”, In *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications (PILBA)*, 12–23.
24. A.D. Thierer, “The Internet of Things and wearable technology: Addressing privacy and security concerns without derailing innovation”, *Richmond Journal of Law and Technology*, 21(2), 2015.
25. R.L. Rutledge, A.K. Massey, and A.I. Antón, “Privacy impacts of IoT devices: A smart TV case study”, In *Requirements Engineering Conference Workshops (REW)*, IEEE International. IEEE, 261–270, 2016.

Chapter 2

IoT Architecture, Applications, Security and Privacy Issues

A. Harini, Manjula Devarakonda Venkata,
Chandra Sekhar Koppireddy, and G. Vijaya Kumar

Pragati Engineering College, Surampalem, Andhra Pradesh, India

2.1 Introduction

The Internet of Things (IoT) is a novel paradigm made up of billions of autonomously communicating objects. The infrastructure of an already-existing network may be used by the IoT to sense, identify, and operate an object remotely. IoT is a cyber-physical model that uses actuators and sensors to enhance accuracy, efficiency, and economic benefit. It has become an emerging domain in various sectors of applications, connecting people to the internet through mobile phones, computers, and laptops. It is the next generation of the internet. The IoT is a collection of things that consists of objects that include different identities over the internet. IoT includes heterogeneous devices due to the combination of virtual and physical components. The IoT devices will be connected wirelessly by using communication technology like Bluetooth, Wi-Fi, etc. The various types of sensors play a significant role in the environment of IoT due to the advancement in technology. Gartner [1] defines IoT as a network of physical objects that includes embedding technology to sense and interact with the external environment and internal states. Syntactically, the IoT term consists of two terms: the first term is

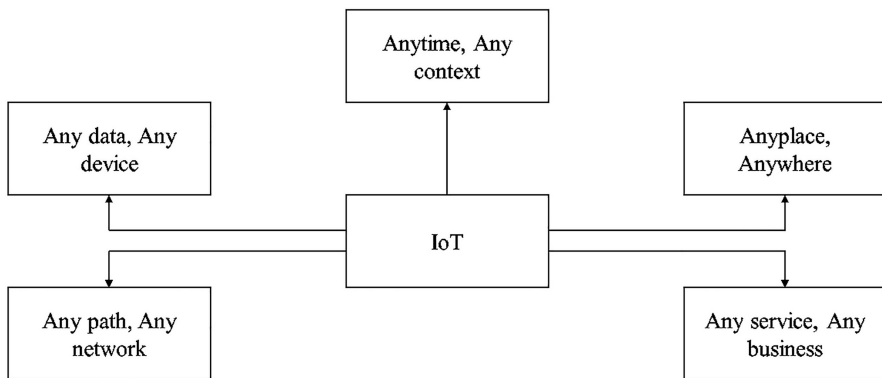


Figure 2.1 Services or connectivity of the Internet of Things.

towards the vision of the network orientation in IoT. Secondly, it focuses on general objects which are integrated into a common framework. The vision of IoT increases from the research, business alliances, stakeholders, and industry by approaching the issues from the perspective of internet-oriented and things oriented.

IoT is also called a global network of smarter objects. IoT refers to creating a network that consists of everyday embedded items with the software, electronics, and communication of the system. The gadgets in the environment of IoT are smaller in size, lower force, and assets the compelled gadgets. The aim of IoT is to utilise intelligent actuators and sensors in order to deliver a ubiquitous experience and a pervasive environment. IoT has the capability of connecting with anyone, anything, at any place, at any time [2] with the network for any type of services as shown in Figure 2.1.

2.2 IoT Architecture

There are generally three different types of architecture in IoT such as three-layer architecture, five-layer architecture, and seven-layer architecture. There is no consent for single architecture in IoT, and it is accepted universally. The basic architecture of IoT includes three layers such as perception, network, and application layers which are shown in Figure 2.2. The three-layer architecture of IoT is developed in the earlier stage of study [3], and it explains the basic idea about IoT. So, the researchers developed an architecture of five layers. The five layers of IoT architecture [4] include the perception, transportation, processing, application, and business layers, as shown in Figure 2.3. The seven-layer architecture of IoT is shown in Figure 2.4.

Perception layer is a physical layer that senses and collects information related to the environment, using actuators, web cameras, sensors, and RFID. Microchips are inserted into objects to improve the sensing and processing capacity, which is necessary for future applications. The critical task in the network layer is to carry

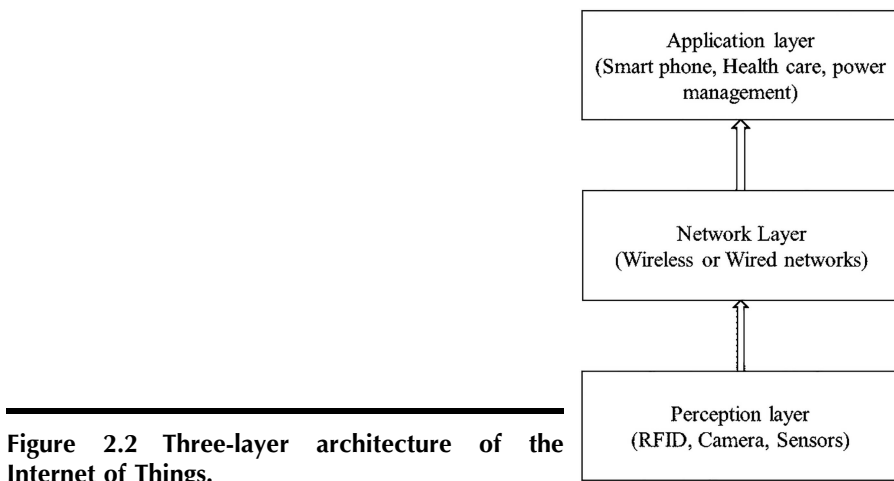


Figure 2.2 Three-layer architecture of the Internet of Things.

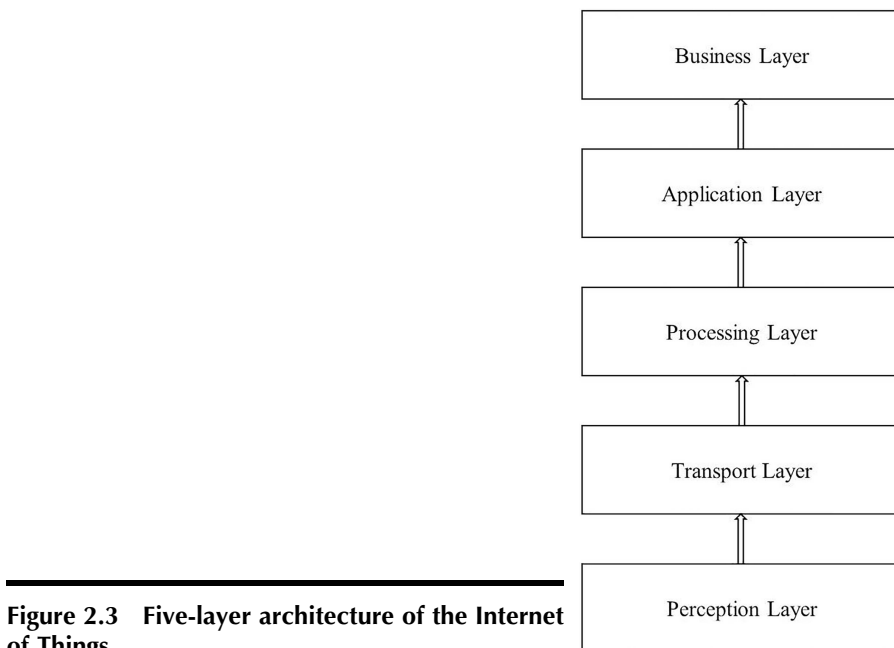


Figure 2.3 Five-layer architecture of the Internet of Things.

out packet routing and host addressing. The network layer routes the information collected from the perception layer. The Internet protocol version 6 is used for addressing the device and for identifying the host address in the hierarchical step. The network layer is responsible for managing the received information from the perception layer. Further, it is responsible for transferring the information to the

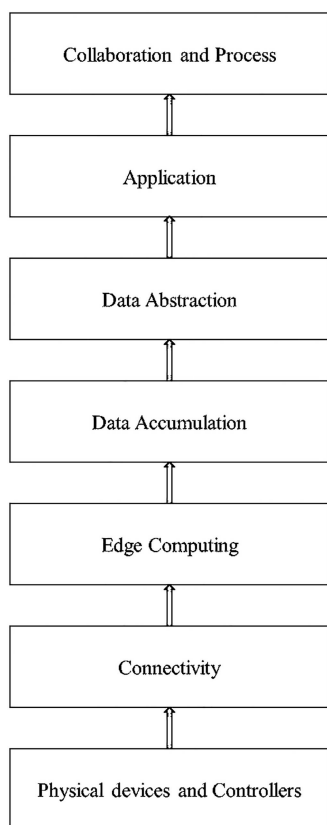


Figure 2.4 Seven-layer architecture of the Internet of Things.

application layer by using different types of network technologies like wired or wireless networks and local area networks. The main path for transferring includes Bluetooth, Wi-Fi, FTTx, ZigBee, infrared technology, UMB, etc.

The application layer provides the interface for interactions with the lower layer of protocol from which the information travels in the network. In the application layer, the data are encrypted and encapsulated, which is achieved by utilising the process-to-process connection in the port. The application layer offers applications that are specific to the service of the users and defines different types of applications in which the IoT is utilised. The application layer provides the necessary tools such as actuating devices for developers to know the vision of IoT.

The processing layer and business layer are further components of the five-layer architecture [5]. Consequently, the perception, transport, processing, application, and business levels are included in the five-layer design. The functionality of the remaining three layers are outlined in the following:

In the transport layer, the end-to-end messages are transported into the network and transfer the sensor's information from the perception layer to the

processing layer by using Bluetooth, Wi-Fi, NFC, etc. The major responsibility of transport layer is segmentation, flow control, and error control. The transport layer carries out a higher quantity of information, so it is necessary to process the enormous amount of data and to provide sound middleware for storage. The network layer technology provides a dynamic and reliable interface to the data that needs to be processed and stored. The transport layer is also called as communication layer as it is responsible for interacting among the middle layer and perception. Every transfer of information will be done securely by keeping the confidentiality of obtained data.

The processing layer is also called the middleware layer, which analyses, processes and stores the huge amount of sensor data that comes from the transportation layer. The processing layer maintains and offers various types of services to the lower layer and uses different technology like cloud computing, big data processing, and database modules. The processing layers stores every dataset, and according to the address and name of the device, it provides specific data to the device. The processing layer includes two responsibilities such as it confirms whether the data is forwarded to authentic users and prevents attackers. The authentication is utilised to check the data and users, and it is applied by using the pre-shared password and keys to the respective users. The second responsibility of the user is to forward the data to the transport layer, and the medium in which the data is transferred among the transport and process layer will be wired or wireless.

The business layer maintains the entire system of IoT by considering the business, application, profit of models, and privacy of users. Business layers [6] are responsible for delivering the tasks such as making graphs, flowcharts, result analysis and improvement in devices, etc. The business layer is referred to as an intended behavior of applications and acts as a manager for the entire system. The privacy of users is maintained by the business layer and can also determine how the information is generated, changed, and stored. The business logic maintains and controls the information exchange among users and the database of applications. The zero-day [7] attack is a problem in the application or security hole which is not known to users.

The seven-layer architecture of IoT is also called multi-layer architecture that includes a perception layer for hosting smarter things, the connectivity for transferring the information from the physical layer to the cloud through networks and gateways. The processing layer uses the platform of IoT for accumulation and managing the entire data streams; the application layer to deliver the solutions in the form of a report, analytics and device control for end-users; the edge computing or fog computing to perform processing of data that are close to the edge and IoT devices collect new information's, and the business layer to make the decision on the basis of information and the security layers which includes every other layer.

2.3 Security and Privacy in IoT

Due to the utilisation of IoT devices in various applications, the security and privacy of users have become a major concern. Cyber threats are increasing explosively by making inadequate for the existing security and privacy measures [6]. Every three minutes, the two devices will be connecting with each other. The exponential growth and connectivity of IoT devices resulted in an increased traffic rate in the network. The security and privacy challenges of user data authentication and verification occurred due to IoT devices' connectivity. The 1 billion Yahoo accounts were composed by hackers in the year 2013, and in 2014, the 145 million eBay users were stacked. In 2017, 143 million customers' personal information from Equifax was stolen. In 2017, 820,000 client accounts were hacked from five billion dollars of the toy industry. The present cyber history shows many disasters in cyber security due to a huge set of data breaches for the flaws of security in billions of microchips and lockdown of computer systems till the payment was made [8]. There are a number of security and privacy challenges increasing day by day among IoT devices. So, the security and privacy in resource-constrained and complex IoT environments are highly challenging and have to be effectively tackled. The machine learning algorithms are utilised to enhance the cyber security system performance and to improve the infrastructure of IoT. IoT has become a significant element for the future internet with the higher rate of applications in business and social life. The larger number of services and applications on IoT are increasing for vulnerable attacks or data theft. Advanced technology is necessary to provide security for the IoT environment against attacks. Data integrity, confidentiality, and authentication, are the major problems based on the security of IoT.

2.4 Security Issues

IoT refers to the larger number of heterogeneous sensor devices that communicate among each other in a local area network over the internet. The threats to IoT differ significantly from the conventional networks due to the limited resource availability of end devices. The IoT devices include lesser computational time and memory, but the traditional internet consists of effective computers and servers with various resources. So, the traditional networks are secured by multiple factors of security layer and complex protocol, which real-time IoT application cannot afford. The IoT devices are less secured with wireless interaction media like ZigBee, 802.11a, LoRa, and 802.15.4. Due to the specific functionality of applications and lack of operating systems, the devices of IoT include various formats and contents of data, making it difficult to establish a standard protocol for security. These limitations leave IoT systems prone to various security issues and privacy threats by opening venues to different kinds of attacks. The probability of attacks increases in the network as the size of the network increase. So, a network of IoT is highly

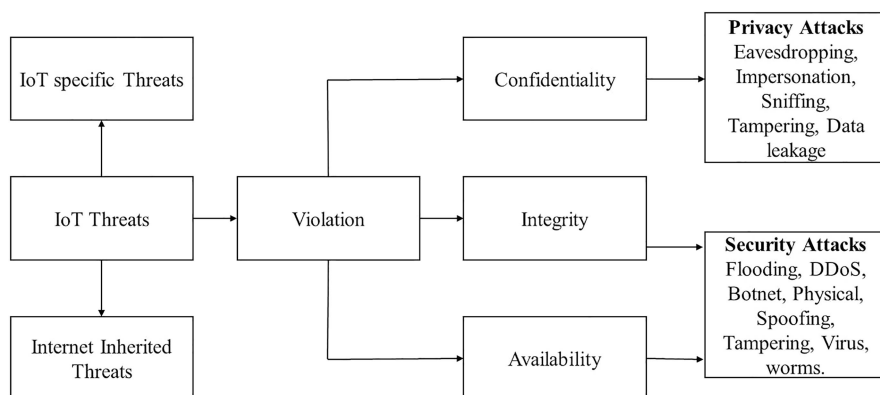


Figure 2.5 Types of IoT threats and violations of IoT threats.

vulnerable compared to a traditional network. The computational resources of IoT devices are lower, so the capacity to deal with advanced attacks is limited. The vulnerabilities of IoT are categorised into common and specific vulnerabilities such as standardisation, battery draining attack, lack of trust for specific IoT devices, and the vulnerability inherited from the internet is considered as the common vulnerability. The types of IoT threats and violation of IoT issues are shown in Figure 2.5.

The issues involved in the service of IoT are privacy, confirmation, reliability, non-revocation, access control, and obtainability. The standard privacy states make the sender alone, and the receiver will have the option to get the message substance. The system of confirmation helps to develop suggestions for characters, and it guarantees to effectively distinguish the beginning of the message. The reliability provides the substance of the message to process it before the recipient shows the data provided by the sender. The non-revocation will not allow the sources to reject the conditions of not sending messages. The access control controls and demonstrates the users who are accessing the data. Finally, the obtainability standards provide the accessibility that is approved by the gatherings of every occasion.

The basic concept of privacy and security revolves about the trio of data confidentiality, data integrity, and network availability. In IoT, the information will be anything such as data of user's identity, packets forwarded from an IP camera to its destination server, commands provided by the users to drive the car utilising multimedia or key fob conversion among the people. The disclosure of information with unauthorised users will violate the confidentiality, integrity, and availability of data. When the threats impact the confidentiality of data, it results in privacy threats. The security threat affects both integrity of data and the availability of the network. The types of IoT attacks are shown in Figure 2.6.

The main goal of the DoS attack is to fill the network with an invalid request which exhausts the resources of the network by consuming the bandwidth of the network, and services will become unavailable for a genuine user. The Distributed

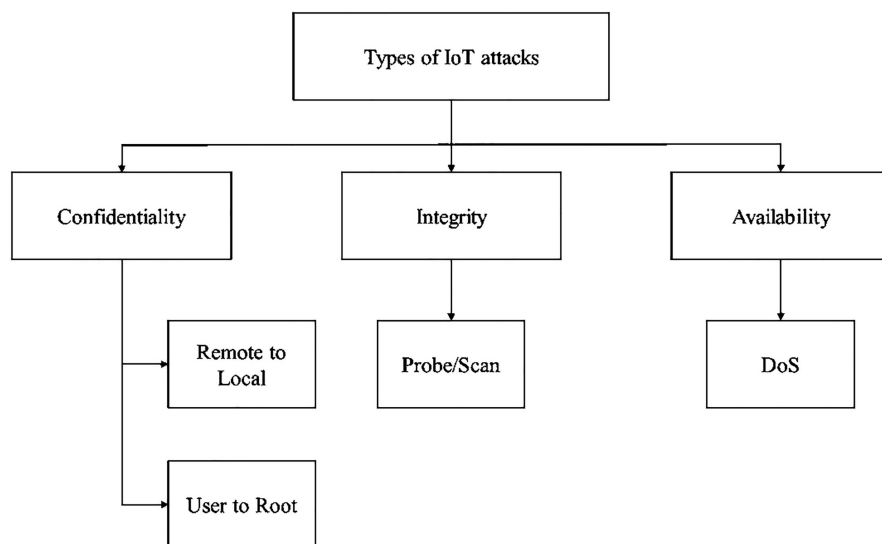


Figure 2.6 Types of IoT attacks based on characteristics.

Denial of Service is an advanced version of the DoS attack in which multiple sources will stack the individual target with more complexity to avoid the attack from being traced. There are several types of DDoS attacks with similar objectives. The variants of DDoS attacks are SYN flooding, where the attackers will forward the SYN requests successively to the targets. The Internet Control Message Protocol (ICMP) attack is where a larger number of packets are forwarded by using the spoofed IP of a victim. The cross-fire attack occurs by utilising a massive and complex larger scale botnet to execute an attack. The UDP with flooding attack sends a higher number of packets to the random ports on the victim of a remote. In the network of IoT, a botnet is the type of DDoS attack where IoT devices are initiated to release the attack on a specific target, such as on a bank's server. The botnet attacks are executed on various protocols such as MQTT and other techniques to overcome the DoS in the environment of IoT.

The Man in the Middle (MitM) attack is the oldest attack in the environment of IoT. Impersonation and spoofing are considered as MitM attack, such as node X planning to interact with the destination B might be interacting with the MitM attackers who will impersonate the B destination. In SSL stripping, the attackers will capitalise the attacks in such a way as to establish a connection with the server by utilising a connection with HTTP. However, the target will not be secured with the HTTP connections. Several research for enhancing the security of MitM attacks were developed, where in the healthcare system the patient will get automatic insulin dosage which is highly vulnerable to MitM attack and results in mortality. The malware is an extension of malicious software, and the increasing

number of IoT devices with patches in the software caused by attackers to install the malware in the devices and perform malicious activity. The malware is in the form of virus, worm, spyware, rootkit, Trojan horse, and malvertising.

In security threats, the users of IoT and their information are vulnerable to privacy attacks like de-anonymisation, sniffing, and inference attacks. The effects are on the data confidentiality in which the data will be at motion or rest. The MitM are classified into active and passive MitM attacks. The passive MitM attack listens to the transfer of data among two devices even if the passive MitM attack violates privacy which will not change the information. The attacker will be having access to the device, which observes silently for months attacking. The increasing number of cameras in IoT devices such as smartphones, wristwatches, and toys affects the passive MitM attack where the sniffing and eavesdropping are more. The active MitM attacks are considered in abusing the information collected from communicating with the people who pretend to be someone else, such as impersonation and accessing the profile without consent.

The data privacy attack is related to MitM attack and is classified as active data privacy attack and passive data privacy attack. The main goal of a data privacy attack is to collect the data from various sources and reveal the target's identity. The attackers will collect the information to impersonate the target of individuals. Finally, the attackers will alter the data by tampering with data classified as active data privacy attacks by re-identifying the data leakage.

The set of actions presents which threatens the confidentiality, integrity, and network availability of the resources. On the basis of characteristics, IoT attacks are classified among four types such as Remote to Local (R2L), User to Root (U2R), Probe or Scan, and DoS attacks.

Confidentiality refers to data not being disclosed or available to unauthorised users for entities or process. The two types of compromising attacks are present under confidentiality, such as R2L and U2R.

R2L attack is the class of attack in which the attackers forward the packets to the machine through the network and then utilises the vulnerability of machines to illegally obtain local access to the machine.

U2R attack is the class of attack in which the users utilise the information about the login of authorised users to provide vulnerability to the network or system.

Integrity refers to the data which is not destroyed or changed in an unauthorised way and is required to provide the reliability for the information, which refers to the capability to give the messages that are not changed.

Probing is the attack that compromises data integrity, and attackers scan the network by collecting the data or finding the known vulnerability.

Availability refers to the system or resources of the system, which provides accessibility and usability by the demand of authorised users of the system. It is the fundamental characteristic of a secured system.

2.5 IoT Applications and Need for Security

The applications of IoT are higher in number because it supports resource-constrained devices and heterogeneous technology. The influence of IoT in every facet of everyday life is due to automatic communications [9] among the devices. Generally, the applications of IoT are classified into enterprise applications and consumer applications. Consumer applications include smart meters, home automation, and wearables. Enterprise applications include monitoring air pollution, smarter warehouse, smarter grid, etc. Smart home, smart buildings, smart healthcare monitoring system, smart cities, and smarter logistics are examples of IoT systems. Figure 2.7 shows several applications of IoT.

Smart Transport: Smart transportation is modernised. The traditional transportations and IoT-based smart transport provide remote unlocking or locking of cars, access traffic information, and download the route map. Further, the vehicles connected with the internet facilitates protection against thefts by immediate alarm messages. The cars, buses, trains, and bicycles are connected by utilising IoT actuators and sensors. The roads also include sensors and tags that gather the data and send it to the controlling center to update traffic and transport the goods.

Smart Buildings: Smart buildings and homes provide efficient power management, controlled by thermostats, sensors, and data analysis algorithms. Home appliances such as washing machines, refrigerators, televisions, and security alarm systems provide computing and services through the internet. Attacks on smarter devices can lead to physical problems.

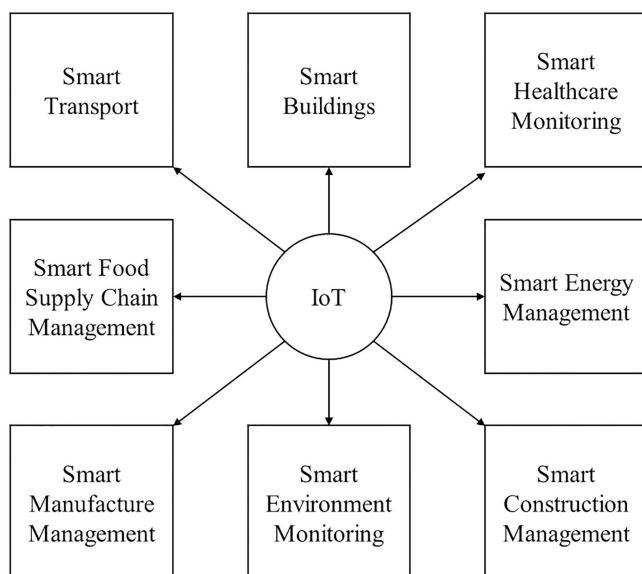


Figure 2.7 Applications of the Internet of Things.

Healthcare Monitoring: Healthcare models are improved by developing signal processing, bio-medical sensing, lower power devices, and wireless communication. Sensors measure blood pressure, temperature, sugar level, and are collected, evaluated, and stored for reference. IoT-based healthcare is developed to provide quick and timely identification of illness. Wearable devices are used to monitor the healthcare system.

Energy Management: The smart systems of IoT are embedded with the electrical application and control the electrical devices such as power outlets, switches that enable the proactive controlling and monitoring of the consumption of energy. The devices are remotely controlled and forward the details to the organisation of electrical supply in order to optimise the power usage in smarter homes and buildings. Furthermore, the advanced metering infrastructure devices are connected with the internet of the electrical company, which not only gathers the data from users and also monitors the automated distributions of devices such as grids and transformers.

Construction Management: IoT is used to manage and monitor infrastructures such as roads, tall buildings, traffic signal towers, aircraft runways, and railway traffic. Smart constructions assist maintenance and construction, repair the schedule, and maintain activity effectively.

Environmental Monitoring: The weather monitoring system with IoT collects humidity, temperature, and pressure information by utilising sensors. The gathered information is forwarded to the cloud and stored in the back ends for visualisation and analysis. In addition, the alert messages are forwarded to users from the applications.

The quality of water and air is evaluated by utilising the devices of IoT, and further, the monitoring of weather is carried out easily. The environmental monitoring system includes different types such as weather monitoring, air pollution monitoring, forest fire, and flood identification which are described as follows: The air pollution monitoring system based on IoT, monitors harmful gases such as CO₂, CO, NO₂, NO, etc. The air pollution control system utilises the meteorological and gaseous sensors that will be installed in the environment and factories.

Manufacturing Management: The smarter devices embedded with the sensors are utilised to monitor the environmental condition and identifies critical conditions such as tremors and floods. The applications need a speed response due to the alarm that is activated immediately in order to provide security.

Smart Food Supply Chain: The IoT provides important details to the executives of the food supply chain. The IoT is utilised already in the management of supply systems, but its benefits are lesser. The noticeable and significant applications of IoT supply chains are the management of security and safety of products by using tracking systems on the basis of IoT. The devices raise the alarm if unauthorised users access the information by breaking the security policy in the supply chain management system.

2.6 Security and Privacy Challenges in IoT

The main challenge in IoT [10] is providing transparent and seamless services without security, as IoT devices' evolution and vast data make them vulnerable to hacking. Hackers can hack IoT devices in just 2 minutes, making it crucial to ensure the security and privacy of IoT applications, as attacks can result in loss of life or disaster.

The development of advanced IoT technologies like software-defined networking, big data analysis, cloud computing, and intelligent sensors has brought about significant advancements. However, these technologies are still in their early stages and face challenges in security and privacy. The heterogeneity of IoT devices increases internet security issues, particularly with personal data, and perimeter defenses are limited in the IoT environment. The security and privacy challenges in IoT are shown in Figure 2.8.

Security: IoT provides opportunities to improve business, but also allows attackers to collect intellectual property, compromise user information, and breach privacy. The existing infrastructure includes the viability of target attacks like ransomware of smart homes, physical injuries, smart cars, data thefts, and novel kinds of botnet to prevent the security issues with the inbuilt security features.

Scalability: The exponential growth of IoT manages the scalability and becomes the important factor that increases the connected devices, application characteristics, users, and analytical capability, which serves through the applications of IoT without affecting the quality of the system. The protection, control, and management of

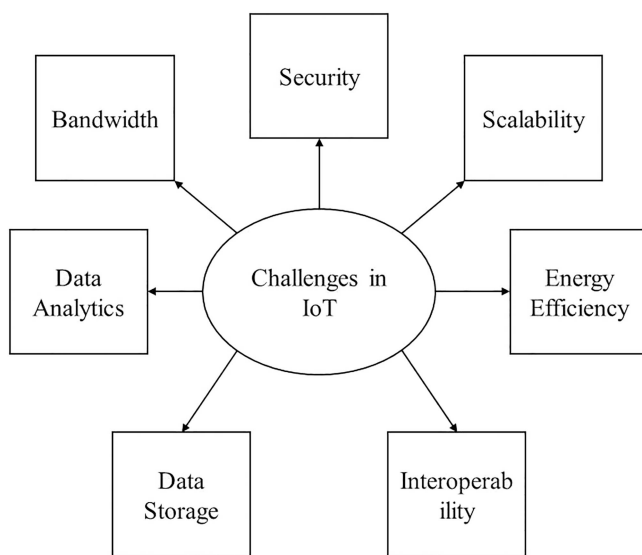


Figure 2.8 Security and privacy challenges in IoT.

increasing the number of devices by the proportions, increases the resources which require the flexible applications of IoT.

Energy Efficiency: Power management will be crucial in the IoT since there will be billions of connected devices. Every gadget in the IoT ecosystem has battery-powered or self-powered sensors instead of relying on the air conditioner gateways and appliances in a home for electricity. The many gateways of functions with the various internet linkages, sensor interface, embedding process, and states to the device that has to be constantly connected into main power or often recharged must manage the power supply. Every device is expected to require solar energy or the use of a solar-charged battery in the future, which reduces the overall amount of energy used by IoT applications.

Interoperability: The IoT infrastructure comprises of many communication and sensor protocols that cope with the diverse environment, ranging from the automotive to the agricultural industries. When using sensors like the Raspberry Pi, Arduino, xsens, and smartec to detect and control the environment by modifying interaction technologies, the IoT devices are connected effectively using a variety of communication protocols including ZigBee, Bluetooth, RFID, and others. For the standard protocols and heterogeneous devices, a capable IoT network architecture is needed.

Data Storage: The IoT tools are utilised by business people to collect information and make effective business decisions to improve customer satisfaction. The collected data are saved and forwarded to a storage system with a specific format which makes the companies replenish the infrastructure of information storage to store the information collected from IoT, which increases the data exponentially and results in adapting the cloud storage for storing the information.

Data Analytics: In various companies, the data analytics of IoT have derived benefits in terms of cost reduction, increased the experience of the customer, reduction of equipment, and productivity of human resources. Even though IoT information is considered valuable, various businesses have not extracted the values from the same data because it will not be aware of present technologies. The information for employees or machines will be overwhelmed when the sensors receive the data in every thirty seconds.

2.7 Conclusion

The IoT is extremely vulnerable to assaults for a variety of reasons, hence security is a need in this setting. The number of IoT devices will first rise, and they will be spread out across both controlled and unmanaged environments. As a result, the attackers will be able to generate assaults using unmanaged devices located far away. However, if the consumers' physical surroundings is hacked, the linked gadgets there will harm them. The IoT then incorporates diverse hardware and software to create the interoperability problem, which opens the door for attackers.

The effects of an assault on the IoT ecosystem extend beyond specific devices, for example, when hacked devices are used in botnets to launch powerful attacks. The detection method or mitigation procedure in IoT is assured to be addressed by the current solutions. Because of this, a protection system that can automatically recognise both known and unknown assaults and defend against them rapidly is necessary given the growing number of IoT devices.

References

1. Gartner Hype Cycle for the year 2019. (Source: <https://www.gartner.com/smarterwithgartner/3-major-trends-drive-gartner-hype-cycle-midsize-enterprises-2019/>)
2. Steve Ranger, "What is the IoT? Everything you need to know about the Internet of Things right now," on February 3, 2020 (Source: <https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/>)
3. Rashmi, "IoT (Internet of Things) Concept and Improved Layered Architecture," *IJEDR*, 6(2), 2018. ISSN: 2321-9939.
4. P. Ramesh et al., "Architecture, Protocols, Layers and Elements of IoT," *IJCRT*, 9(9), September 2021. ISSN: 2320-2882.
5. Marco Lombardi et al., "Internet of Things: A General Overview between Architectures, Protocols and Applications," *Information*, 12, 87, 2021. 10.3390/info12020087.
6. K. Singh and D. D. Singh Tomar, "Architecture, Enabling Technologies, Security and Privacy, and Applications of Internet of Things: A Survey," *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, ISMAC 2018, 642–646, 2019. 10.1109/ISMAC.2018.8653708.
7. V. Sharma et al., "A Framework for Mitigating Zero-day Attacks in IoT," 1–4, 2018. [Online]. Available: <http://arxiv.org/abs/1804.05549>.
8. J. Zhang et al., "Middleware for the Internet of Things: A Survey on Requirements, Enabling Technologies, and Solutions," *Journal of Systems Architecture*, 117(5), 102098, 2021. 10.1016/j.sysarc.2021.102098.
9. K. Shaukat et al., "A Review on Security Challenges in Internet of Things (IoT)," *The 26th IEEE International Conference on Automation and Computing (ICAC'21)*, September 2–4, 2021. 10.23919/ICAC50006.2021.9594183.
10. M. S. Virat et al., "Security and Privacy Challenges in Internet of Things," *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, 454–460, 2018. 10.1109/ICOEI.2018.8553919.

Chapter 3

Current Trends in IoT Data Management: An Investigative Study

Kattu Jahnavi, Addanki Snehitha Naga Sai Lalitha, and Manas Kumar Yogi

CSE Department, Pragati Engineering College (A), Surampalem, Andhra Pradesh, India

3.1 Introduction

Internet of Things (IoT) Data Management is a great combination which is effectively used by all organizations. The IoT is famous for connecting various devices. We use sensors, physical devices, etc. From home appliances to industry, IoT plays a vital role. Data Management adds an advantage for IoT. Data Management manages vast amounts of data. As many devices are involved in IoT we have to deal with a large amount of data. Database deals with them and manages the data. It provides security for data. It also maintains information about the data being captured by sensors and makes it useful for further purposes. IoT data management is used in different fields like health care, industrial automation, agriculture, environmental monitoring and transportation. IoT data management involves efficiently handling and utilizing data generated by IoT devices. It involves addressing challenges like data volume, velocity, variety, and veracity to derive value from IoT data.

3.1.1 Components of IoT

The components of IoT tell us how [1] we build a completely successful IoT device. Below are a few concepts which are involved in building IoT devices.

1. **Things/Devices:** sensors contain different physical objects or devices that are embedded into them, actuators, and connectivity capabilities. They can range from not only simple household objects but also objects like thermostats and light bulbs to complex industrial machinery.
2. **Sensors and Actuators:** Sensors capture data from the surrounding places, such as temperature, humidity, pressure, or motion. The sensors are used to sense the changes and give signals to the corresponding system or device.
3. **Processing of Data:** IoT devices collect vast amounts of data which need to be processed, analyzed, and converted into meaningful perception. To make this happen we use different algorithms and techniques to extract valuable information, detect patterns, and make data-driven decisions.
4. **Cloud Computing:** Cloud platforms play a key role in IoT by providing scalable storage and computing power. They have features which deal with the storage and processing of large amounts of data generated by IoT devices and also enable remote access and control.
5. **Security and Privacy:** Data by Day IoT device usage has been expanding. Ensuring the security and privacy of data becomes critical. More concern is taken in terms of security because it is the most required thing. IoT is best at providing these security and privacy aspects.

3.1.2 Applications of IoT

IoT has a wide range of applications across various industries and sectors [2] including: (Figure 3.1)

1. **Smart Homes:** IoT is used in many household activities. The television is an IoT-based device. All the devices are given sensors from vehicles to even hand wash which clearly shows the application of IoT.
2. **Industrial Automation:** IoT usage in the industry can optimize industrial processes by monitoring equipment performance, predicting maintenance needs, and improving operational efficiency.

IoT – A network connecting several devices. It connects the world. IoT uses several devices, sensors, and technologies.

3.1.3 Data Management

Data management is the practice of organizing, storing, and processing data in a structured and controlled manner to ensure its integrity, availability, and usability.

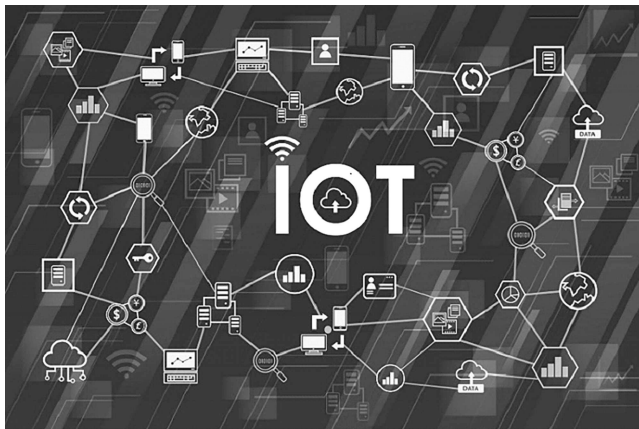


Figure 3.1 Spectrum of IoT.

It involves various processes, technologies, and strategies to handle data throughout its lifecycle, from creation to archival or deletion.

3.1.4 Components of Data Management

1. **Data Governance:** Data governance refers to the framework and processes for managing and controlling data. It involves defining policies, procedures, and guidelines for data management, establishing data ownership and accountability, and ensuring compliance with regulations and standards.
2. **Data Quality Management:** Data quality management focuses on maintaining the accuracy, consistency, and reliability of data. It includes processes for data cleansing, validation, de-duplication, and data profiling to identify and resolve data quality issues.
3. **Data Integration:** Data integration calls for data from different devices and combines the data to get the wanted result to observe. It includes techniques like data extraction, transformation, and loading (ETL), as well as data integration tools and platforms.

3.1.5 Applications

Data management involves defining the lifecycle of data from creation to deletion. It includes processes for data retention, archival, and disposal following legal, regulatory, and business requirements. Overall, effective data management is essential for organizations to leverage data as a strategic asset [3].

1. **Business Intelligence and Analytics:** Data management plays a critical role in business intelligence and analytics, enabling organizations to collect, store,

clean, integrate, and analyze data to gain insights and make informed decisions. It involves data warehousing, data modelling, ETL processes, and data governance to support data-driven decision-making.

2. **Customer Relationship Management (CRM):** Data management is essential in managing customer data and supporting CRM initiatives. It involves capturing, organizing, and analyzing customer information, such as interactions, preferences, and purchase history, to enhance customer satisfaction, personalize marketing efforts, and improve customer retention.

These are the few applications regarding data management.

3.1.6 IoT Data Collection and Storage

A few main steps involved in data management are as the chapter name tells Data Collection, Data Storage, and Data Integrity. Let's start understanding this concept.

3.1.7 Data Collection

Until now we have discussed what data management is and what is IoT and all. Now as in our day-to-day life, we need data for many other processes to be done. Whatever the process might be we Google it, we apply the data we gather on that task and we finally get the result based on the data we collect. The data which we obtain through the source are filtered and based on the final result we will decide whether the outcome is good or bad.

Similarly, as humans, IoT also takes data as input through sources and makes many filterings by passing the data through different layers and finally the data will give an accurate result.

For example, the latest trend smart watch is used by many people [4]. There are many kinds of features in a smart watch; similarly it contains a pulse rate checker, stress rate checker and many others which are related to health and this smartwatch collects all the data and runs its algorithm in its backend and provides the resultant output.

Data collection plays a crucial role in IoT data management. The collected data may hold sensor readings, environmental data, location information, machine status, and other relevant metrics (Figure 3.2).

This five-layer architecture's role is to store, analyse and process the information received from its corresponding layer. In the working of the above layers, the technology also involves other components like database, cloud computing, etc.

3.1.8 Data Storage

Data storage involves all kinds of data which are collected and stored in the cloud or edge for long or short-term applications. The functionalities provided in Edge,

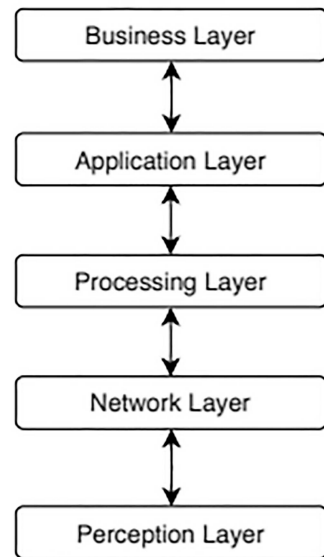
5-Layers

Figure 3.2 The five-layer architecture.

are sensor data aggregation, pre-processing of the data, and securing connectivity to the cloud. The cloud provides various database management systems built for IoT applications. The systems can manage those enormous amounts of data for further applications.

Examples of storage support are DBMS, Edge Storage, etc.

3.2 Stream Processing in IoT Data Management

Stream processing in IoT data management refers to the ability to collect, analyze, and derive actionable insights from data in near real-time as it is generated by IoT devices. [5] This allows organizations to make immediate resolutions and take timely activities based on present and future updated information.

Here are the key aspects of real-time data processing and analytics in IoT data management:

1. **Data Collection:** IoT devices frequently produce a vast volume of data from various sensors and sources. Real-time data processing involves collecting this data in real-time, often through streaming technologies, and ingesting it into a centralized system for analysis.

2. **Data Preprocessing:** Before analysis, real-time data needs to be preprocessed to ensure its quality and relevance. This involves performing tasks such as data cleansing, normalization, and transformation to remove noise, handle missing values, and ensure consistency.
3. **Real-time Analytics:** Once data is collected and preprocessed, real-time analytics techniques are applied to extract meaningful insights. This can include real-time statistical analysis, anomaly detection, pattern recognition, predictive modelling [5], and machine learning algorithms.
4. **Edge Computing:** To reduce latency and enable faster processing, real-time data analytics can be performed at the edge of the network, closer to the IoT devices. Edge computing platforms allow for real-time analysis and decision-making at the edge, reducing the reliance on centralized cloud systems.
5. **Visualization and Reporting:** Real-time data analytics is often complemented with intuitive visualizations and dashboards to provide real-time insights to stakeholders. Real-time reporting capabilities enable the monitoring of key metrics, trends, and anomalies in real time.

3.3 Security and Privacy in IoT Data Management

3.3.1 Security in IoT Data Management

Security in IoT data management is of utmost importance due to the sensitive nature of the data and the potential consequences of security breaches. Several key aspects need to be considered to ensure robust security in IoT data management. Firstly, device security is critical. IoT devices often have limited resources and may lack built-in security features. Implementing [6] strong authentication, secure boot mechanisms and regular firmware updates can help protect against unauthorized access and mitigate the risk of device-level vulnerabilities.

Secondly, data encryption plays a vital role in safeguarding IoT data. Access control mechanisms are crucial for IoT data management. Role-based access control, multi-factor authentication, and fine-grained access policies can help ensure that only authorized individuals or systems can access and manipulate the data. Regular access reviews and audits are necessary to identify and address any potential security gaps.

3.3.2 Types of IoT Device Security

IoT device security can be implemented in different ways. IoT consumers can deploy network-level security solutions, while IoT manufacturers can integrate embedded IoT security into the devices (Figure 3.3).

The immense challenges of IoT security

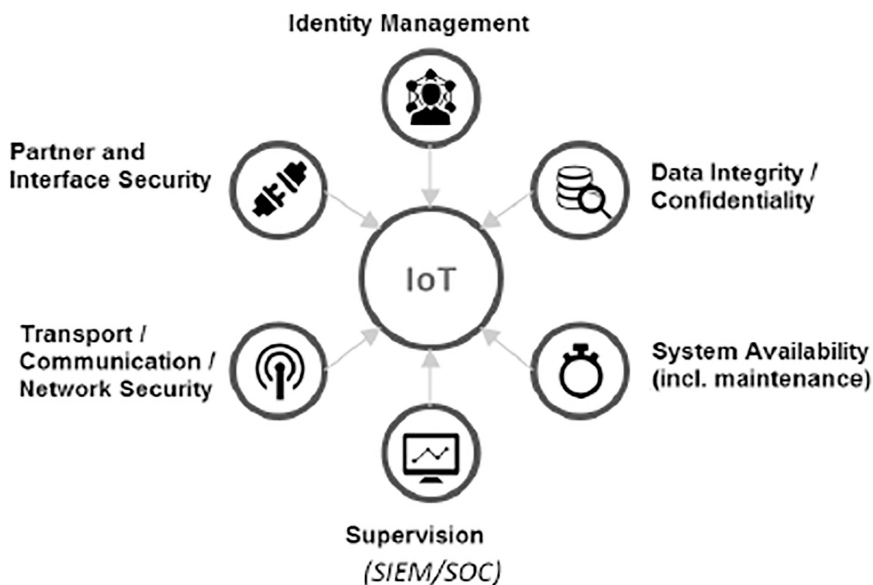


Figure 3.3 The immense challenges of IoT security.

1. **Network Security in IoT:** Routing traffic to and from IoT devices through a network security appliance, IoT device owners can monitor and can control traffic to their devices. By a deep understanding of IoT protocols and threats, IoT network solutions can identify and can block attempted exploits before they reach vulnerable IoT devices.
2. **On-Device Embedded Security:** Manufacturers can embed securities to integrate IoT devices. Embedded IoT security is installed within the firmware of IoT devices and provides runtime protection for these devices against cyber threats [7]. Firmware IoT security uses instrumentation to monitor the state of binaries on the device as they run. This deeper visibility enables firmware security solutions to identify and reinforce attempted attacks based on identifying and preventing even novel IoT exploits.

Security is an important topic in every sector similarly in IoT also every layer needs security for privacy (Figure 3.4).

3.3.3 Privacy in IoT Data Management

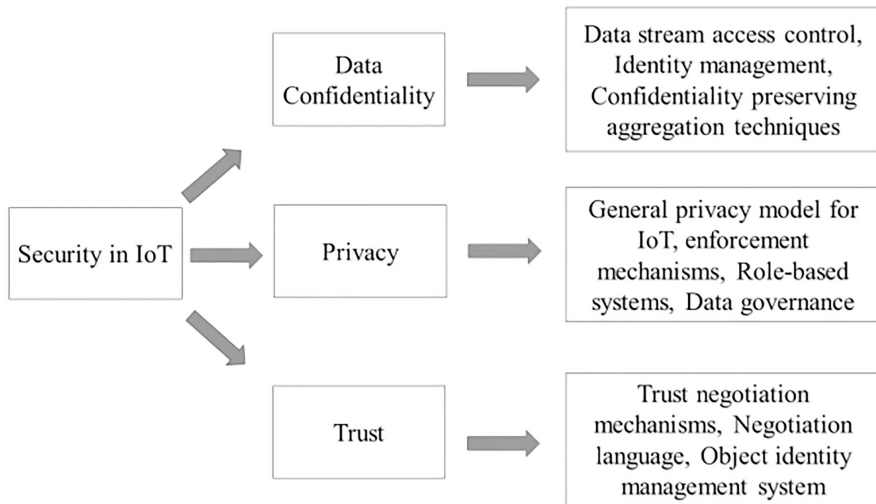


Figure 3.4 Security in IoT.

3.4 Data Visualization and Reporting

Data visualization and reporting play a crucial role in IoT data management by providing meaningful insights and facilitating decision-making processes. Here's an overview of [8] data visualization and reporting in IoT data management.

3.4.1 Data Visualization

Data visualization involves presenting data in an illustrated or visual format to make complex information more understandable and accessible. Data visualization helps in (Figure 3.5):

1. **Understanding Data Patterns:** Visual representations such as charts, graphs, and maps help in identifying patterns, trends, and correlations within IoT data. This allows stakeholders to gain insights quickly and make data-driven decisions.
2. **Real-time Monitoring:** Visualization dashboards provide real-time updates and visual indicators to monitor IoT devices, sensors, and systems. This enables stakeholders to track the status, performance, and health of IoT deployments in real time.
3. **Identifying Anomalies:** Visualizing data in real-time allows for the detection of anomalies and outliers that may indicate system malfunctions, security

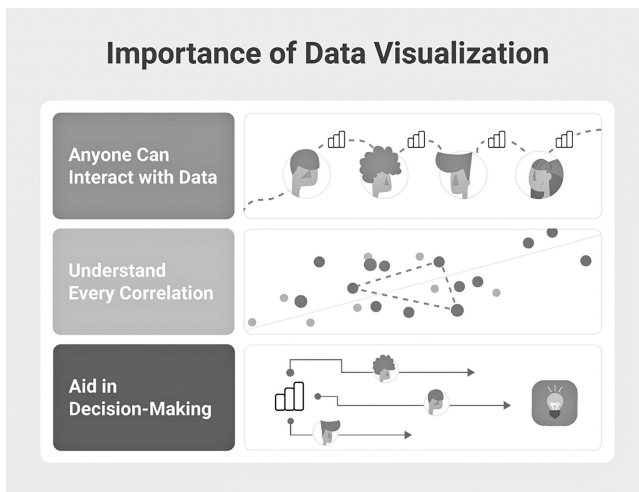


Figure 3.5 Importance of data visualization. Visualization makes understanding easy because it involves pictures which do not need to be explained.

breaches, or unusual behaviour in IoT devices. Visual alerts and notifications can help stakeholders take immediate action.

3.4.2 Data Reporting

Data reporting involves generating and [9] distributing reports based on analyzed IoT data. Reporting in IoT data management serves the following purposes:

1. **Performance Monitoring:** Regular reports on key performance indicators (KPIs) help monitor the performance of IoT systems, devices, and processes. These reports provide insights into metrics like uptime, response times, throughput, and resource utilization.
2. **Compliance and Auditing:** Reports can be generated to demonstrate compliance with industry regulations, standards, and data privacy laws. These reports document data handling practices, security measures, and adherence to governance policies.
3. **Predictive Maintenance:** Reports generated from IoT data analysis can provide insights into equipment health, maintenance schedules, and failure predictions. This allows organizations to proactively plan maintenance activities, reduce downtime, and optimize asset utilization.

The combination of effective data visualization and reporting in IoT data management empowers stakeholders to understand and leverage the insights derived from IoT data.

3.5 IoT Data Monetization and Business Models

3.5.1 Monetization and Business Models in IoT Data Management

Monetization and business models in IoT data management refer to the strategies and approaches that organizations adopt to generate revenue and [1] create value from the IoT data they collect and manage. Here are some common monetization models and business strategies in IoT data management

1. **Data-as-a-Service (DaaS):** Organizations can offer data as a service by providing access to their IoT data to external parties. These data be in the form of raw data feeds, pre-processed data streams, or curated datasets. Customers can leverage this data for their analysis, research, or development of new products and services.
2. **Subscription-Based Model:** Organizations can charge a recurring fee for providing access to real-time IoT data, analytics, or insights. Customers pay a subscription fee to access and utilize the organization's IoT data management platform, which may include data visualization tools, reporting capabilities, and additional services.
3. **Value-Added Services:** Alongside the provision of IoT data, organizations can offer value-added services that leverage the data to deliver additional benefits to customers. This can include data analytics, predictive insights, personalized recommendations, or consulting services to help customers derive actionable insights from the IoT data.
4. **Data Monetization:** In some cases, organizations may anonymize and aggregate IoT data to protect privacy while extracting valuable insights. They can then sell these aggregated and anonymized datasets to third parties, such as researchers, marketers, or data-driven companies, who can leverage the data for various purposes like market analysis, trend identification, or research studies.

3.6 Future Trends and Case Studies in IoT Data Management

3.6.1 Future Trends in IoT Data Management

The field of IoT data management is constantly evolving, and several future trends are shaping its trajectory. The key trends that are expected to have a significant impact:

Edge Computing: As the volume and velocity of IoT data continue to increase, there is a growing need to process and analyze data closer to its source. Edge computing brings computation and analytics capabilities closer to IoT devices, reducing latency and bandwidth requirements. This trend allows for real-time

decision-making and enables organizations to extract valuable insights from IoT data at the edge of the network.

Data Security and Privacy: With the proliferation of IoT devices and the potential for data breaches, ensuring data security and privacy is of utmost importance. Future trends in IoT data management will focus on implementing robust security measures, [4] such as end-to-end encryption, secure authentication protocols, and data anonymization techniques. Organizations will also need to comply with evolving data protection regulations and build trust with users by being transparent about data collection, usage, and storage practices.

Blockchain Technology: Blockchain has the potential to address several challenges in IoT data management, including data integrity, security, and trust. Blockchain can provide a decentralized and tamper-proof ledger for recording IoT data transactions, ensuring transparency and immutability. It enables secure data sharing and facilitates trust among multiple stakeholders in IoT ecosystems.

3.7 Case Studies in IoT Data Management

3.7.1 *Precision Agriculture and Crop Management IoT Data Management*

One prominent case study in precision agriculture and crop management utilizing IoT data management is the collaboration between John Deere and The Climate Corporation's FieldView platform. FieldView integrates data from various sources such as weather stations, satellite imagery, soil sensors, and John Deere's farm equipment. This data is processed and analyzed to provide farmers with valuable insights and recommendations. Farmers can access real-time monitoring, receive alerts for changing weather conditions, and track field operations remotely. The platform offers intuitive visualizations, enabling farmers to monitor crop growth, assess yield potential, and identify areas that require attention. Additionally, FieldView facilitates data-driven benchmarking, allowing farmers to compare their performance with regional averages or similar fields. The integration of John Deere's farm equipment ensures seamless data transfer and synchronization, capturing relevant information on planting, spraying, and harvesting activities. Overall, this case study exemplifies how IoT data management enhances precision agriculture, enabling farmers to optimize resource allocation, improve productivity, and contribute to sustainable farming practices.

3.8 Conclusion

In conclusion, this chapter provided an overview of IoT data management and explored various factors involved in IoT data management, including data

collection, storage, integration, analysis, visualization, and security. IoT data management is good adaptability for today's organizations'. As modernization will be increased in the future, everything will be connected to IoT. Sensors will be used even in small sectors. The tools the technologies used by IoT data management are more effective which can make the work of humans very easy [2]. This makes us not observe everything the sensors will capture the things and send the signals. The data will be stored in the database and we can use the data security and privacy is maintained highly. The consistency of the data is maintained. No unauthorized users can make use of it. As IoT will be the most preferable technology which will evolve and increases its importance in the world. With the emerging techniques of data management strategies, usability also increases and makes IoT effective to use.

In conclusion, IoT data management is a crucial discipline that empowers organizations to harness the transformative potential of the IoT ecosystem. By effectively managing IoT data, organizations can derive valuable insights, make informed decisions, and unlock the full potential of the connected world [10].

References

1. Science soft. <https://www.scnsoft.com/case-studies/penetration-testing-of-mobile-iot-apps-and-smart-security-cameras>
2. Bahga, A., and Madisetti, V. (2014). Internet of Things: A hands-on approach. Vpt.
3. Lansdale, T., Bloodsworth, P., Anjum, A., and McClatchey, R. Querying the Future Internet. *Proceedings of 1st International Workshop on Database Architectures for the Internet of Things*. <https://www.mdpi.com/1424-8220/13/11/15582>.
4. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376.
5. Luo, C., Wu, F., Sun, J., and Chen, C.W. Compressive Data Gathering for Large-Scale Wireless Sensor Networks. *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom 2009)*. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0ddc8ee97d4ca2822fff642257e01ac10cfda8c2>
6. Privacy and security of IoT Author: Dean Ivancevic Supervisor: David Randall Examiner: Associate Professor Päivi Jokela. <http://www.diva-portal.org/smash/get/diva2:1504361/FULLTEXT01.pdf>
7. Diao, Y., Ganesan, D., Mathur, G., and Shenoy P. Rethinking data management for storage-centric sensor networks. *Proceedings of the Third Biennial Conference on Innovative Data Systems Research (CIDR 2007)*. http://web.mit.edu/tibbetts/Public/CIDR_2007_Proceedings/papers/cidr07p03.pdf
8. IoT ethics must factor into privacy and security discussions Dr Laetare Cybersecurity LLC. <https://www.techtarget.com/iotagenda/opinion/IoT-ethics-must-factor-into-privacy-and-security-discussions>

9. Ethical Data Management in the Age of The IoTShareShareBy Special GuestMark Coggin, senior director of solutions marketing at Red Hat. <https://www.iotevolutionworld.com/magazine//features/articles/429360-ethical-data-management-the-age-the-iot.htm>
10. Santos, M.G., Ameyed, D., Petrillo, F., Jaafar, F., and Cheriet, M. (2020). Internet of Things Architectures: A Comparative Study. ArXiv, abs/2004.12936. https://www.researchgate.net/profile/Marcela-Santos/publication/340962806_Internet_of_Things_Architectures_A_Comparative_Study/links/5eb9d8f44585152169c82c71/Internet-of-Things-Architectures-A-Comparative-Study.pdf

Chapter 4

A Study on the Impact of Internet of Things Development and Future Spectrum

He Yigang¹, Farhan Ali², Chengweiding², and Ait Mouha Radouan²

¹*School of Electrical Engineering and Automation, Wuhan University, Wuhan, China*

²*School of Electrical Engineering and Automation, Hefei University of Technology, Hefei, China*

4.1 Introduction

Internet of Things (IoT) is expected to generate an estimated trillion dollars in revenue in the coming years [1]. The IoT is a staggering and fast-expanding field: major technological advances of the 21st century, such as machine-to-machine (M2M) communication and the impending IoT, are sparking a connectivity revolution that will radically disrupt many industries.

Management of radio frequencies (or “spectrum”) is an approach to regulate use to maximize efficiency and maximize net social benefit [2–8]. Managing the IoT spectrum effectively is essential for achieving the entire premise of the IoT. Four steps used in IoT spectrum deployment: (1) **spectrum allocation**: Governments and

regulatory bodies allocate specific frequency, typically reserved for low power, short-range wireless communication for licensed and unlicensed spectrum. (2) **spectrum management:** After spectrum allocation, it needs to manage and ensure communication without interference by enforcing regulations and monitoring spectrum use to maximize spectrum efficiency. (3) **network architecture:** IoT devices need specialized architecture to enable reliable and efficient communication. (4) **Device compatibility:** IoT devices must be designed with specific band allocation. It may require careful attention to software development, hardware design, and regulatory issues. The current most significant challenge is spectrum allocation, which is insufficient to support the growing number of IoT devices, especially in urban areas where the spectrum is congested. This congestion can lead to interference, reduced data rates, and reliability issues. Despite the challenges, the IoT spectrum presents several opportunities. One opportunity is the potential for dynamic spectrum access. Dynamic spectrum access allows IoT devices to share the spectrum with other wireless technologies by opportunistically accessing unused frequencies, leading to more efficient spectrum usage and better spectrum utilization. Another opportunity is using new wireless technologies such as LoRa and Sigfox. These technologies use unlicensed spectrum and provide low-power, long-range communication, making them suitable for IoT applications such as smart cities and agriculture. These technologies can also complement existing wireless technologies, allowing for better spectrum utilization and harmonization. The Future development will resume assessing the blooming of spectrum demand for IoT, focusing on sub-1GHz bands. It is unnecessary to allocate and designate bands for IoT. Access to more spectrum for IoT may be facilitated in various ways, including via IoT-enabling technical harmonization steps and a specific authorization framework. Specifically, the Industry is seeking a portion of the frequency spectrum between 800 and 900 MHz for use in non-licensed activities (e.g., for smart metering, smart home applications). Spectrum harmonization measures for short-range devices to handle the many types of IoT in this frequency range, giving preference to pre-existing license-exempt bands and bands providing economies of scale and international harmonization. There are many methods by which access to more spectrum for the IoT may be enabled. These include the implementation of technical harmonization measures that will allow IoT functionality, as well as the establishment of a dedicated authorization system. The Industry is actively pursuing a designated segment of the frequency spectrum ranging from 800 to 900 MHz for non-licensed purposes, such as smart metering and smart home applications. To effectively manage the many types of IoT devices operating within a specific frequency range, it is necessary to implement spectrum harmonization procedures. These methods prioritize the utilization of pre-existing license-exempt bands and bands that provide economies of scale and international harmonization.

The question is if the licensed spectrum available for commercial wireless services or slated for allocation is sufficient to serve the IoT; how to guarantee that adequate spectrum is known beyond the bands being examined for commercial

wireless connectivity and how it will cover the cost, including alternate bands that may be suited for the IoT; if frequency sharing that is not currently achievable for other forms of commercial wireless networks may support the development of the IoT; the function and spectrum might be need of IoT applications and services delivered by satellites; What regulatory constraints may prevent spectrum availability for IoT implementation, including buildout requirements for IoT networks, licensing regions, license terms, and conditions? The significance of unlicensed devices in expanding the IoT and whether sufficient spectrum is/will be available for such activities. The current spectrum allocation is limited, and IoT devices need to coexist in the spectrum with other wireless technologies. IoT future applications such as smart homes, wearables, and industrial automation are already changing how we interact with technology.

Figure 4.1 describes the IoT spectrum in detail, the frequency testbed development of IoT. However, their success depends upon the availability of a reliable and efficient spectrum. The radio spectrum allocated for IoT is scarce, necessitating IoT devices' coexistence with other wireless technologies like Wi-Fi, cellular, and Bluetooth; in the previous decades, challenges associated with the IoT. Spectrum has a limited availability of frequencies, which was insufficient to support

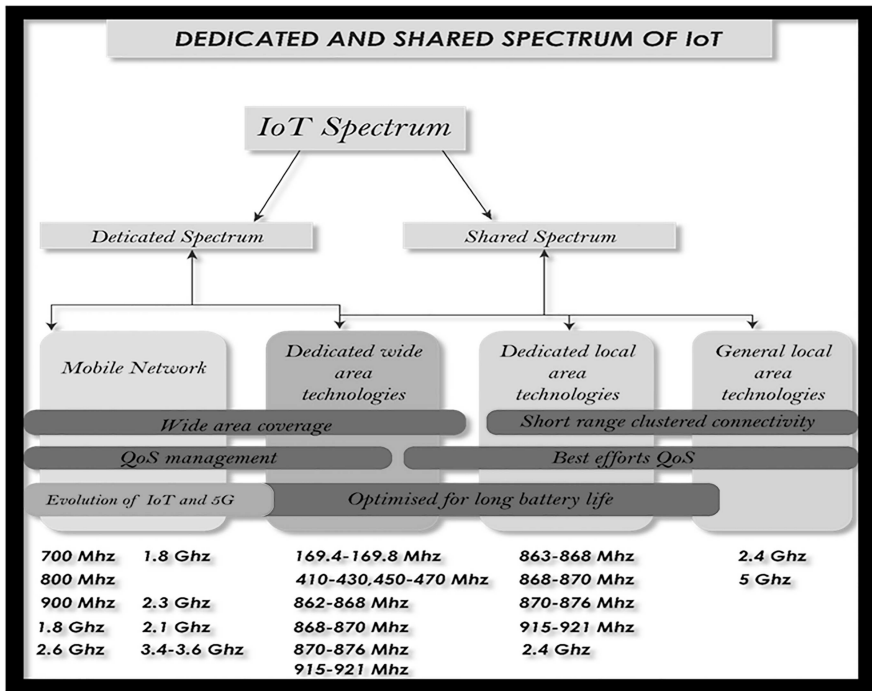


Figure 4.1 Internet of Things spectrum frequencies.

Table 4.1 Technological Challenges, Opportunities, and Concerns

<i>Year</i>	<i>Technologies</i>	<i>Opportunities</i>	<i>Challenges</i>	<i>Concerns</i>
2000	Rfid, Wireless Sensor network, Zigbee	Logistics, military	High Cost, limited connectivity	Security, privacy
2010	Low energy, Bluetooth, 4G, and cloud computing	Retail and industrial IoT	Data management, interoperability	Cybersecurity, data privacy
2020	5G, AI/ML, Edge Computing	Energy management	Standardization, deployment, complexity	Cybersecurity, data privacy. data security, data ownership

the growing number of IoT devices, especially in urban areas where the spectrum is congested. This congestion can lead to interference, reduced data rates, and reliability issues. Security is one of the most important issues consistent with IoT every decade (Please see Table 4.1). Table 4.1 describes that for the last 2 decades, IoT has had security and privacy concerns every decade. With the upgradation of technology, security and privacy concerns are constantly part of every technology like RFID, wireless sensor networks, AI, edge computing and so on.

Table 4.1 describes the evolution of IoT challenges and opportunities; the critical challenge of the IoT can be considered as heterogeneous and comes in different shapes, sizes, and power requirements, like low-data-rate communication and low power. At the same time, others may require high-data-rate communication and high power. The heterogeneity will make it more challenging to design and deploy future spectrum allocation schemes that may satisfy all the requirements. This sharing poses several challenges that need to be addressed to enable the full potential of IoT. The limited availability of frequencies is also a crucial challenge for the IoT spectrum.

The development and growth of IoT will bring challenges for their associated technologies like Sensor Actuators, RFID, NFC, WIFI, Bluetooth, ZIGBEE, Z-wave, Lora-Wan, NB-IoT, APIs, SDK, platforms, Protocols, Middleware, Network connectivity, Artificial intelligence, Edge Computing, Data processing, Cloud Computing, big data, Cloud computing, Authentication encryption, Access control, User interface and so on. Table 4.2 describes future spectrum challenges with their associated technologies, problems, and solutions in reference.

Table 4.2 Future Challenges of IoT with Their Possible Solutions

<i>Future Challenge</i>	<i>IoT Associated Technology</i>	<i>Solution</i>
Security	Authentication, encryption, firewall, access control	Security protocols are updated regularly, and analysis and real-time monitoring, risk assessment, and management strategies
Scalability	Artificial intelligence, big data, and cloud computing	AI-powered resources allocation, analytics, scaling with cloud computing and distributed systems
Interoperability	API standards, middleware, and common communication protocols	Integration platforms, communications gateways and bridges, and standardization of protocol
Privacy	Secure data storage, informed consent, and privacy-enhancing technologies	Anonymization, user control data sharing, and user privacy policies
Reliability	Recovery system, backup, and fault tolerance redundancy	Disaster recovery strategies, predictive maintenance, and continuous monitoring
Power management	Communication networks, energy-efficient sensors, and devices	Optimization of energy harvesting, renewable energy sources, and battery management
Complexity	Intelligent systems, automation, and a simplified user interface	Automated configuration, simplified application development tool, and user-friendly interface
Cost	Cloud services, communication, modules, and low-cost sensors	Shared Infrastructure, economies of scale, standardization of components

4.1.1 Future-Specific Applications and Examples of IoT

Several IoT future industry applications that will be fully applicable shortly are smart homes (smart thermostats, innovative security systems, bright lighting, and smart speakers), industrial IIOT (remote monitoring, predictive maintenance, and asset tracking), Healthcare IOT (remote patient monitoring, smart pills dispensers, and wearable health tracker), agriculture IoT (intelligent irrigation systems, animal monitoring, and soil sensors), smart cities (smart waste management, public safety systems, and smart traffic management), transportation (fleet management system, autonomous vehicles, and connected cars), retail IoT (smart shelves, personalized marketing, and Beacon technology). Emerging technologies need global economies of scale, where the spectrum is readily available in its current form. Bands for mobile cellular networks, such as those being examined for 5G, are included in this category for short-range devices (like WIFI) and low-power WANs. Nonetheless, the need for spectrum access rises with the proliferation of IoT applications. In contrast, the quantity and quality of spectrum access demanded will vary significantly according to operational requirements and use cases, even though there is a wide variety of data rates, dependability, range, and output power. IoT has expanded significantly, and many spectrum options are available for various use cases, including multiple applications and operating needs. Unprecedented uses will provide new harmonized usage requirements for the IoT.

Nonetheless, a shared emphasis on the bands in this road plan might permit further economies of scale when they are only attainable nationally. A mix of general and specific spectrum licensing is necessary to ensure enough spectrum access for IoT devices. No one authorization structure or set of technical constraints for spectrum access would accommodate all feasible needs. IoT spans more applications and use cases than mobile cellular networks currently permit. Frequencies that have been authorized or reserved have the potential to be utilized for emerging IoT services and applications. In accordance with the principle of technological neutrality, it is imperative to ensure that existing standardized technical solutions align with those designed for the IoT. One challenge comes in informing IoT stakeholders about the many spectrum access options.

4.2 IoT Standards and Framework

In this section, we are going to discuss several IoT protocols and frameworks, encompassing 6LoWPAN, ZigBee, OneM2M, DDS (Data Distribution Service), LiteOS, AWS IoT, ARM Mbed IoT, AMQP (Advanced Message Queuing Protocol), Microsoft's Azure IoT Suite, CoAP (Constrained Application Protocol), Google's Brillo/Weave Calvin, among others. In this discussion, we shall talk about a select handful.

4.2.1 6LoWPAN

IEEE 802.15.4 is used as the foundation for 6LoWPAN technology's low-power wireless network system [9–12]. Incompatibilities exist between the IPv6 format and the forms approved by IEEE 802.15.4., so although it may seem straightforward to construct a data packet of a wireless or wireless sensor network, it is not. Due to 6LoWPAN's ability to smooth out these differences, 802.15.4 may be used as a layer on top of the system. To send IPv6 packet data via 6LoWPAN, the data must be converted into a format the IEEE 802.15.4 lower layer system can accept. According to the IPv6 standard, it is mandated that the Maximum Transmission Unit (MTU) should possess a minimum size of 1,280 bytes. The current size of 127 octets exceeds the maximum limit specified by the IEEE802.15.4 standard for packet size. This standard was implemented to restrict broadcast length and minimize power consumption. IPv6 nodes are given hierarchical 128-bit identifiers to overcome the address resolution issue. Once the devices have established a connection, the IEEE 802.15.4 devices can utilize either IEEE 64-bit extended or 16-bit addresses that are unique inside the Personal Area Network (PAN). PAN-IDs are assigned to groups of IEEE802.15.4 devices that are close to one another. Interoperability is a fundamental standard concern. Various manufacturers' gear must work together. All architectural layers must be compatible to verify interoperability, which is a great issue. To guarantee this, many standards apply. Every component may be evaluated for standard compliance and compatibility. 6LoWPAN is a wireless / IoT standard gaining momentum. Initially developed for the IEEE 802.15.4 standard, this technology can operate with alternative wireless protocols, rendering it suitable for various applications. The utilization of IPv6 in 6LoWPAN provides it with a distinct advantage. Adopting IPv6 on a global scale has led to several benefits offered by 6LoWPAN in the context of low-power wireless sensor networks and other similar networks with limited power resources.

4.2.2 Zigbee

Zigbee uses IEEE Standard 802.15. Zigbee is based on IEEE 802.15.4 for control and sensor networks (WPANs). Zigbee WPANs operate at 2.4 GHz, 900 MHz, and 868 MHz. The Zigbee Alliance maintains and updates the Zigbee standards, which add network and security layers to the IEEE 802.15.4 standard. The alliance's standards enable multivendor interoperability. Custom application developers who don't need to work with other programs may design their versions and extensions. Zigbee PRO, RF4CE, and IP are the current standards. Zigbee PRO supports low-cost, dependable device-to-device networks for IoT. Zigbee PRO delivers Green Power, a new feature that enables self-powered or energy-harvesting devices. Zigbee RF4CE is designed for use in situations requiring bidirectional control between devices but not mesh networking. Zigbee IP improves IPv6-based wireless mesh networks to manage low-power, low-cost

devices. Zigbee Alliance simplifies wireless product integration to enable manufacturers to offer energy-efficient wireless control sooner and more cost-effectively. Members of the alliance work to create public standards for wireless communication that is reliable, secure, low-power, and simple to use. Organizational structures such as committees, work groups, study groups, task forces, and SIGs organize the alliance. ZigBee and Wi-Fi share the 2.4 GHz spectrum [13,14]. Wi-Fi and ZigBee must be carefully planned to avoid interference in the same surroundings. ZigBee and Wi-Fi on the same frequency will interfere. ZigBee is usually affected.

4.2.3 OneM2M

Connectivity enables machine-to-machine connections and the IoT. Soon, even the simplest gadgets will be linked [15,16]. The oneM2M framework encompasses components of comprehensive IoT systems, including end-point devices, sensors, and data visualization tools. Additionally, it incorporates IoT gateways, platforms, and interfaces that provide seamless integration with non-oneM2M sub-systems. It's used in smart manufacturing, cities, and households. Consider a linked plan to show oneM2M, end-to-end M's architecture, and standardization in complex and dynamic systems. This particular use case demonstrates the integration of interconnected devices, the transmission of data to a centralized dashboard, and the implementation of a control application. The OneM2M usage scenario can extend its interoperability to encompass additional urban installations. This architecture comprises Application Entities(AE), Interworking Proxy Entities (IPE), and Common Service Entities (CSEs). Autonomous entities (AEs) refer to interconnected equipment and applications integrated with sensors. Artificial entities (AEs) may be found in devices that offer user applications and services, such as dashboards and analytics. These AEs, also known as Apps, establish a connection with oneM2M by utilizing REST APIs. Interoperability entities (IPEs) establish a functional interface between legacy devices and the oneM2M service layer standard. The IPEs facilitate converting oneM2M and non-oneM2M protocols and data models. The oneM2M standardization effort facilitates interoperability among a wide range of widely adopted technologies. Illustrative instances encompass interfaces designed for industrial Programmable Logic Controllers (PLCs) such as Modbus and interfaces tailored for smart home devices like ZigBee. The oneM2M service layer is implemented in gateways, servers, and certain high-capacity consumer devices, commonly called CSEs. This layer offers IoT data and connectivity services.

4.3 IoT Architecture

IoT architecture helps administrators manage IoT devices. IoT gadgets gather data using tiny sensors and relay it to a server. Servers process data to provide

business insights. This data is utilized to automate operations that increase system uptime and efficiency. IoT design ensures that data is sent and handled properly. Without adequate IoT design, networks will be unstable, undermining the point of IoT. It is significant that throughout the inception and subsequent development of the IoT, scholarly papers and researchers have consistently emphasized examining IoT architecture. Several authors have described the three-layer architecture, which consists of the application, network, and perception layers. Others described four layers: the semantic layer, service layer, pattern layer, and network layer. A limited number of authors have portrayed a framework consisting of five distinct layers: perception, middleware, application, business, and network. Simultaneously, certain levels were delineated, including but not limited to the application, network, transport, 6lopan, and data link layers [17]. Consider the scenario we classify published scholarly research layers [17–26]; in this scenario, we will become acquainted with various layers of the IoT, including the Internet layer, adaptation layer, things layer, network layer, transport layer, sensing layer, business layer, internet or decision layer, support and action layer, link layer, session layer, transmission layer, router/hub layer, cloud layer, messaging layer, middleware layer, service-oriented architecture (SOA) layers, and object-oriented layer. In a scholarly work, the author examined the seven-layer architecture of the IoT while incorporating a two-layer framework for enhancing security and privacy [27]. The three-layer approach is straightforward but leaves out critical facts about data utilization. Below, we will cover the IoT architecture and implementation issues. According to academics, the structure and classifications of the IoT vary. Testbed creation and deployments [23] consider the IoT's third-through-sixth-layer architecture. Four separate yet functionally equivalent layers make up the IoT's defining architecture. Each layer's function and importance are explained next.

4.3.1 Perception Layer

The perception layer represents IoT devices. Health monitoring, illumination, autonomous cars, robots, and security systems are examples. Each IoT gadget gathers data. Cheap IoT sensors can handle hundreds of data points. The data gathered depends on the organization's aims. Agricultural IoT devices can record weather, moisture, temperature, and airflow to boost crop output and profitability.

4.3.2 Transport Layer

Transport sends data to the cloud or edge device for processing. The transport layer utilizes internet gateways to facilitate data transmission from the physical layer to the processing layer. Administrators use cellular and Wi-Fi networks to transfer data. Admins may employ many technologies at this level.

4.3.3 4G LTE/5G Wi-Fi Bluetooth LPWAN

Administrators may combine transport protocols for IoT architecture. The transport protocol you pick should consistently allow sensor-to-internet gateway data.

4.3.4 Processing Layer

The server may turn data into information once it reaches the cloud or edge device. Modern IoT designs analyze data using machine learning and AI. If an IoT sensor records a high-temperature fluctuation, AI may alert to this anomaly by comparing the current temperature to the baseline. In this scenario, the server may send a command to an HVAC unit to reduce the temperature. Humans must inform the server what to do when particular rules or thresholds are satisfied. Administrators handle IoT device orchestration, rule settings, and SLAs at the application layer. Reliable IoT designs to control and maintain their networks via an application layer dashboard; centralizing IoT networks minimize complexity, improving efficiency and security.

4.3.5 Business Layer

The business layer transforms information into business intelligence that drives decision-making. Application-layer insights help stakeholders and executives make better business choices. Business information is provided through reports and live dashboards. Integrations at this level may augment application-layer data. Business intelligence analysts may compare power use before and after installing smart lighting sensors to determine cost efficiency.

Furthermore, the three, four, and five layers of the IoT architecture did not consider security and the privacy layer. The security and privacy layers [27] are also crucial. Rather than specifying the two levels, each of the four levels must be responsible for its privacy and security and be highly responsive to threats independently [28]. For IoT, a standardized architecture is important. This transformation requires a sort of mobile communication that is robust and dense. This innovative technology will enable the next generation of linked devices, including autonomous vehicles and intelligent sensors. The design incorporates many radio access protocols, including GSM, Wi-Fi, and LTE.

The IoT will profoundly impact the standards and protocols governing Internet-connected devices and mobile connectivity shortly [29,30]. Internet services will reach attainable improvements and successes. For low-power, massive machine-to-machine, and human-to-machine communication, it is necessary to develop new protocols. This decade will see indoor communication's greatest prevalence, facilitating interaction between diverse IoT-described devices and communication circumstances.

4.4 Future Advancements

The introduction of 5G technology has brought about a substantial revolution in the architecture of the IoT. The advent of 5G technology has resulted in various advancements that have significantly influenced the implementation of IoT technologies. A number of the key features involved the incorporation of network slicing, which enabled the creation of tailored virtual networks intended to support certain IoT applications. This technological development has enabled optimizing resource allocation, improving Quality of Service (QoS), and efficient management of many IoT applications. Furthermore, integrating edge computing in deploying 5G technology is a substantial and noteworthy accomplishment. The decrease in latency was accomplished by facilitating data processing and analysis at the network's periphery, in immediate proximity to the data origin. The integration of this invention has enabled the effective usage of real-time and essential IoT applications, such as industrial automation and autonomous vehicles. The incorporation of 5G NR (New Radio) technology has substantially impacted the IoT structure, providing improved connectivity, decreased energy usage, and the capacity to connect numerous devices.

Consequently, it has enabled broad IoT ecosystem advancement and proliferation. The continuous development of the technological environment gives rise to conjecture about the structure of the 6G IoT, offering intriguing perspectives on prospective forthcoming progressions. Although detailed information regarding 6G technology is lacking, predicting potential patterns or advancements is feasible. The possible implementation of Terahertz frequency support shows promise in enabling higher data rates and improving spectrum utilization efficiency. The ongoing advancements in the domain of edge computing possess the capacity to augment the processing capabilities of IoT devices, thereby enabling the execution of intricate artificial intelligence (AI) and machine learning (ML) operations at the edge. The potential rise in popularity of decentralization and distributed architectures could facilitate peer-to-peer communication among IoT devices. This transformation can yield enhanced scalability, reduced latency, and heightened fault tolerance for networks pertaining to the IoT. The emergence of 6G technology presents an opportunity to address the growing security and privacy concerns. One potential area of advancement lies in developing encryption techniques, which may include integrating quantum communication to enhance data protection to an unprecedented level. The significance of guaranteeing the integrity of IoT ecosystems requires using secure device onboarding and strong authentication protocols. Building upon the concept of speculation, the 7G IoT architectural framework can redefine the boundaries of connectivity and cognitive skills. Implementing ultra-low latency communication can build a dominant standard, enabling immediate and seamless exchanges across various devices and applications. This advancement would reveal possibilities for seamless

collaboration between human beings and automated systems. The potential for substantial breakthroughs exists by combining artificial intelligence (AI) with the IoT. This involves enhancing equipment with the capacity to autonomously make decisions using advanced machine learning models. As a result, this integration can reduce reliance on centralized cloud resources. In a hypothetical future scenario, it is conceivable that energy harvesting and wireless charging technologies could potentially attain noteworthy levels of efficiency, hence augmenting the self-reliance and sustainability of IoT devices. The evolutionary process can create a worldwide setting in which ordinary objects seamlessly integrate into an ecosystem distinguished by “ambient intelligence.” The notion of ambient intelligence pertains to a technologically advanced environment that can adapt intelligently and intuitively to the presence of humans and their interactions with technologies. The potential of this phenomenon to greatly alter our interactions with technology and profoundly influence our daily routines and experiences is noteworthy. While widespread speculation exists on the potential designs of 6G and 7G IoT systems, it offers an intriguing glimpse into the potential opportunities. Adopting connectivity and technology in global society leads to advancing IoT design in successive wireless network generations. This advancement has the potential to bring about significant changes in various sectors, enable the development of innovative applications, and ultimately shape the course of human existence in ways that are currently unpredictable. The IoT is diverse, including various applications and operating needs. There is no one option for spectrum access that satisfies all of these usage cases since their technical requirements, even though there is a wide variety of data rates, dependability, range, and output power. IoT has already expanded significantly, and there is currently a multitude of spectrum options available for various use cases. Nonetheless, the need for spectrum access rises in tandem with the proliferation of the IoT applications, while the precise quantity and quality of spectrum access demanded will vary greatly according to operational requirements and use cases. The RSPG will resume assessing the blooming of spectrum demand for IoT, focusing on sub-1GHz bands. It is unnecessary to allocate and designate bands for IoT. Access to more spectrum for IoT may be facilitated in various ways, including via IoT-enabling technical harmonization steps in a specific authorization framework. Specifically, the Industry is seeking a portion of the frequency spectrum between 800 and 900 MHz for use in non-licensed activities (e.g., smart metering, smart home applications). Spectrum harmonization measures for short-range devices to handle the many types of IoT in this frequency range, giving preference to pre-existing license-exempt bands and bands providing economies of scale and international harmonization. A deployment in these bands presents a significant policy challenge, as other users of the spectrum (such as government and railway communications) may have legitimate concerns and need to be protected; this means that it must consider their problems. Bands for mobile cellular networks,

such as those being examined for 5G, are included in this category, as are bands for short-range devices (like WiFi) and low-power wide-area networks. Unprecedented uses, such as RUPNs for confined areas, are emerging. (For example, in hospitals, industries, smart factories, and the Utility business), will provide new harmonized usage requirements for the IoT. PMR and utility customers continue to thrive in demand spectrum availability for using creative new technologies and other purposes. For Industry, proposals have been made in the framework of the 800–900 MHz frequency band's harmonization effort. A complementary combination of generic and individual spectrum authorization will be required to guarantee that IoT devices have access to the spectrum. No one authorization structure or set of technical constraints for spectrum access would accommodate all feasible needs. IoT spans more applications and use cases than mobile cellular networks currently permit. 5G will allow new IoT use cases since particular IoT functionality will be incorporated into 5G from the beginning, with capabilities such as network slicing, low energy usage, and scalability.

The rapid and extensive growth of the IoT presents many intricate difficulties that require resolution. The significance of cybersecurity cannot be exaggerated. The susceptibility of IoT networks to breaches, data theft, and unauthorized access is attributed to the interconnection of multiple devices within these networks. Implementing encryption, authentication, and continuous monitoring strategies is crucial to protecting sensitive data and upholding user privacy. The implementation of these security measures is vital in effectively reducing the risks that are linked with them. Another noteworthy challenge that necessitates attention is the matter of interoperability and standards. Implementing IoT devices and platforms involves several communication protocols, which presents difficulties in data exchange and collaboration. Standardization is pivotal in promoting interoperability, easing integration across different platforms, and potentially resulting in vendor lock-in, advancing a more cohesive and efficient IoT ecosystem. The magnitude of data produced by the IoT is significant. Numerous businesses encounter difficulties efficiently handling, storing, and analyzing substantial quantities of data. The attainment of efficient data utilization and latency reduction must establish a harmonious equilibrium between edge processing and cloud analytics. The significance of energy efficiency cannot be overemphasized. A considerable number of IoT devices exhibit constraints in terms of power sources, hence requiring inventive approaches to enhance battery life and preserve energy. To enable the deployment of IoT networks, it is crucial to develop components that exhibit minimal power consumption, energy-harvesting techniques, and intelligent power management systems. The advent of the IoT carries substantial ramifications for both societal and ethical considerations. The concerns surrounding user consent, data ownership, and algorithmic biases arise due to the prevalent practice of extensive data collecting. Establishing comprehensive legal frameworks and observing ethical principles are crucial for efficiently managing the

IoT expansion and achieving a harmonious equilibrium between technical advancement and the safeguarding of individual rights. The IoT harbours considerable potential, yet it also entails notable challenges. To effectively leverage the capabilities of the IoT and develop a dependable, interconnected, and ethically sound digital environment, it is crucial to consider certain fundamental elements. The factors mentioned above encompass cybersecurity protocols, the capacity for devices and systems to function together seamlessly, efficient procedures for managing data, considerations for energy efficiency, and the settlement of societal issues.

4.5 Conclusion

In this chapter, we discussed the IoT as seeing significant growth and emerging as a disruptive phenomenon, reshaping many industries and daily interactions. This is achieved by promoting interconnectivity between devices through IoT infrastructure. The architectural foundation of the IoT encompasses a diverse range of communication technologies, each specifically tailored to address certain use cases and discusses various spectrum solutions, particularly 6LoWPAN, Zigbee, and OneM2M, which offer alternate connectivity options for a wide range of applications. In standards of IoT, 6LoWPAN and Zigbee technologies are renowned for their energy-efficient and extensive coverage attributes, while Zigbee is acknowledged for its proficiency in mesh networking capabilities. Establishing standards and frameworks for the IoT is crucial in ensuring IoT ecosystems' interoperability, scalability, and security. The advancement toward future networks will provide enhanced data speeds, decreased latency, and increased device density, enabling real-time applications and more complex IoT deployments.

Furthermore, it is important to acknowledge the presence of significant challenges that persist alongside these accomplishments. Cybersecurity threats remain very significant, primarily due to the escalating popularity of the IoT. The IoT progress has revealed susceptibilities, requiring robust encryption, authentication, and intrusion detection protocols. Prioritizing data privacy and resolving ethical problems are crucial for developing and retaining public confidence in IoT technology. Moreover, it is essential to address the challenges associated with interoperability that emerge from the extensive implementation of multiple standards and protocols to avoid the development of isolated ecosystems. The concept of the IoT encompasses a dynamic setting wherein various components, including spectrum architecture, standards, and frameworks, converge to establish a future defined by interconnectedness. To effectively use the transformative potential of the IoT in fostering creativity, optimizing productivity, and improving overall well-being, it is crucial to adopt proactive strategies for addressing the challenges that inevitably emerge, notwithstanding the multitude of advancements and opportunities at hand.

Funding: This work was supported by the National Natural Science Foundation of China under Grant No. 51977153, 51977161, 51577046, the State Key Program of the National Natural Science Foundation of China under Grant No. 51637004, the national key research and Development plan “important scientific instruments and Equipment development” Grant No.2016YFF0102200, Equipment research project in advance Grant No.41402040301.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not ApplicableThe authors have no conflict no interest regarding this Book chapter.

References

1. J. Reed, M. Vassiliou, and S. Shah, “The role of new technologies in solving the spectrum shortage [point of view],” *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1163–1168, 2016.
2. O. Monye, “Legal rights of users in the light of the Internet of Things (IoT): A Nigerian perspective,” *Journal of Commercial and Property Law*, vol. 4, no. 1, pp. 25–41, 2016.
3. S. K. Das *et al.*, “Comprehensive review on ML-based Ris-enhanced IoT systems: Basics, research progress and future challenges,” *Computer Networks*, vol. 224, p. 109581, 2023.
4. X. Wang, Q. Chen, and X. Yu, “Research on spectrum prediction technology based on B-LTF,” *Electronics (Basel)*, vol. 12, no. 1, p. 247, 2023.
5. T. K. West and C. O. Johnston, “Efficient parametric uncertainty analysis of an Earth entry vehicle concept using least angle regression,” in *AIAA SCITECH 2023 Forum*, p. 2430, 2023.
6. M. Wolfram and M. Kienesberger, “Gender in sustainability transition studies: Concepts, blind spots and future orientations,” *Environmental Innovation and Societal Transitions*, vol. 46, p. 100686, 2023.
7. U. A. Haider, M. Noman, A. Rashid, H. Rmili, H. Ullah, and F. A. Tahir, “A semi-octagonal 40-bit high capacity chipless RFID tag for future product identification,” *Electronics (Basel)*, vol. 12, no. 2, p. 349, 2023.
8. M. A. S. Sejan, M. H. Rahman, M. A. Aziz, D.-S. Kim, Y.-H. You, and H.-K. Song, “A comprehensive survey on MIMO visible light communication: Current research, machine learning and future trends,” *Sensors*, vol. 23, no. 2, p. 739, 2023.
9. D. Guiducci, C. Carciofi, V. Petrini, *et al.*, “Sharing under licensed shared access in a LTE real test network at 2.3–2.4 GHz,” in *Proceedings 27th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications*, Spain, September 2016.
10. C. Jie and G. Ming, “Performance analysis of star topology wireless sensor networks based on IEEE 802.15.4 [J]”, *Tsinghua University (Science & Technology)*, vol. 55, no. 5, pp. 565–571, 2015.
11. Z. Shelby, and C. Bormann, *6LoWPAN: The wireless embedded Internet [M]*, John Wiley & Sons, 2011.

12. Z. Honggang, S. Chen, and Z. Leyu, "Design and implementation of lightweight 6LoWPAN gateway based on Contiki," *2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, pp. 1–5, 2018. 10.1109/ICSPCC.2018.8567741.
13. K. Nomura and F. Sato, "A performance study of ZigBee network under Wi-Fi interference," *2014 17th International Conference on Network-Based Information Systems*, pp. 201–207, 2014. 10.1109/NBiS.2014.86.
14. C. Seneviratne and H. Leung, "A low complex spread spectrum scheme for ZigBee based smart home networks," *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 984–987, 2016. 10.1109/CCNC.2016.7444923.
15. C. Gezer and E. Taşkın, "An overview of oneM2M standard," *2016 24th Signal Processing and Communication Application Conference (SIU)*, pp. 1705–1708, 2016. 10.1109/SIU.2016.7496087.
16. N. Chaabouni, M. Mosbah, A. Zemmari, and C. Sauvignac, "A oneM2M intrusion detection and prevention system based on edge machine learning," *NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–7, 2020. 10.1109/NOMS47738.2020.9110473.
17. R. Kanagavelu and K. M. M. Aung, "A survey on SDN based security in Internet of Things," in *Advances in Information and Communication Networks*, K. Arai, S. Kapoor, and R. Bhatia, Eds, vol. 887. Cham: Springer, 2019.
18. A. Ghaffarian-Hoseini *et al.*, "The essence of future smart houses: From embedding to adapting to sustainability principles," *Renewable & Sustainable Energy Reviews*, vol. 24, no. 1, pp. 593–607, 2013.
19. S. Greengard, "Smart transportation networks drive gains," *Communications of the ACM*, vol. 58, no. 1, pp. 25–27, 2015.
20. G. Pan *et al.*, "Trace analysis and mining for smart cities: Issues, methods, and applications," *IEEE Communications Magazine*, vol. 121, no. 6, pp. 120–126, 2015.
21. M. Amin and W. Bruce, "Toward a smart grid: Power delivery for the 21st century," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, 2005.
22. D. X. Li, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.
23. J. Gubbi *et al.*, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
24. Z. Liu, K. K. R. Choo, and M. Zhao, "Practical-oriented protocols for privacy-preserving outsourced big data analysis: Challenges and future research directions," *Computer Security Journal*, vol. 69, pp. 97–113, 2017.
25. A. L. L. Atzori, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
26. L. Li, "Study on security architecture in the Internet of Things," in *Proceedings 2012 International Conference on Measurement, Information and Control*, pp. 374–377, 2012.
27. F. Ali, H. Yigang, and R. Yi, "A novel security architecture of Internet of Things," *International Journal of Computer Theory and Engineering*, vol. 11, no. 5, pp. 89–96, 2019.
28. S. H. Mousa, M. Ismail, R. Nordin, and N. F. Abdullah, "Effective wide spectrum sharing techniques relying on CR technology toward 5G: A survey," *Journal of Communications*, vol. 15, no. 2, pp. 122–147, February 2020.

29. G. Shi, Y. He, B. Li, L. Zuo, B. Yin, W. Zeng, and F. Ali, "Analysis and modeling of wireless channel characteristics for Internet of Things scene based on geometric features," *Future Generation Computer Systems*, vol. 101, pp. 492–501, 2019.
30. G. Shi, Y. He, Y. Zhang, B. Yin, and F. Ali, "Detection and determination of harmful gases in confined spaces for the Internet of Things based on cataluminescence sensor," *Sensors and Actuators B: Chemical*, vol. 296, 126686, 2019, ISSN 0925-4005, <https://doi.org/10.1016/j.snb.2019.126686>.

Chapter 5

Revolutionizing Retail: IoT Applications for Enhanced Customer Experience

Ushmita Gupta¹, Pritesh Somani¹, Nitesh Behare¹,
Rashmi Mahajan¹, Meenakshi Singh¹, and
C.A. Vishwanathan Iyer²

¹*Balaji Institute of International Business, Sri Balaji University, Pune, Maharashtra, India*

²*Assistant Professor, Balaji Institute of International Business, Sri Balaji University
Pune, Maharashtra, India*

5.1 Introduction

(Clark, 2021) In today's dynamic retail landscape, where customer expectations are rapidly changing, the amalgamation of technology has become domineering for businesses to become competitive and deliver exceptional customer experiences. A retail experience where physical encounters and digital technologies combine to improve one another is known as phygital, a recent concept. Digital technology enhances physical channels, while humanizing digital channels. An encounter that is more unique and interesting is the end result. (Leszek Marek, 2017) Internet of Things (IoT), One of the most transformative technologies has made a significant contribution in reshaping retail industry by empowering connectivity between

physical objects and the digital world. Technology advancements like the IoT present new management and scientific difficulties as well as opportunities for business and study. There is now more information available to managers about their customers thanks to the system of object communication. (Pan Wang, 2015) Moreover, IoT applications are revolutionizing the way retailers engage with customers, personalize experiences, and optimize operations. The potential of IoT in retail drives beyond mere automation. The IoT is evolving into a new type of industrial information architecture that is used to streamline information flows among global supply chain networks. It comprehends an extensive array of applications, from augmenting customer engagement and streamlining operations to collecting and analyzing valuable data towards offering actionable insights. By harnessing the power of IoT, retailers can create immersive and seamless experiences that may lead to consumer delight at every touchpoint. In the current era of intense competition, businesses need to embrace technology to foster innovation in their service models and provide the best of the customer experiences. As revolution in the IoT endures to reveal, forward-thinking business are exploring the potential of IoT solutions to enrich customer service. According to Forbs (2021), 56% of companies are aggressively investing in IoT to improve customer experience whereas 42% of companies have already started implementing personalized services through IoT. It holds substantial potential for augmenting business operations and driving revenue growth in the business. When it comes to ‘customer experiences’, IoT offers unified platform of data management which deals with both buyers and sellers with timely information and also endowing them to make informed decisions.

(Shotwell, 2022) Payment is a vital part of closing the gap between online and offline buying experiences. The consumer experience is made more convenient and dependable by the ability to accept a variety of digital payment options. For both online and offline shoppers, it might be more convenient to accept purchase now pay later, QR code payments, virtual payments like Google Pay and Apple Pay, as well as cryptocurrency. Because of this, fintech innovation and the retail industry are tightly intertwined. The easier it is for a retail company to plan the efficient functioning of online and offline stores regarding the financial aspect, the more economical and efficient the solutions given by fintech companies are.

5.2 Introduction to the Retail Industry

In modern societies, retail industry plays significant role in bridging a gap between manufacturers and the final consumer. It incorporates a wide range of businesses, comprising e-commerce platforms, brick-and-mortar stores, boutiques, supermarkets, and many more. Retailers are accountable for sourcing, warehousing, distributing, and selling goods and services to meet consumer’s demand. In last few years post the pandemic, consumer along with point of contact both have undergone substantial technological transformations and rigorously changing consumer behaviour. On the

other hand, rise of e-commerce platforms, proliferation of mobile devices, and the multifold demand for personalized experiences have created major disruption across the traditional retail models. Traditional retailers the well-known mom and dad stores have been facing challenging situations like fierce competition, changing customer expectations, and simultaneously the need to deliver seamless and engaging shopping experiences to customers every single time they undertake their shopping experience (Gupta). The retail sector is always evolving to stay competitive in the dynamic and unstable business environment of today. Successful retailers are those who have the flexibility to adapt to their surroundings, create new customer-serving strategies, and do so while respecting the dynamics of current trends.

5.3 Overview of IoT

The term IoT was first proposed by Kevin Ashton in 1999 (Pradyumna Gokhale, 2018). It has emerged as a disruptive technological force which has huge potential to revolutionize industries across the board, including the retail sector too. IoT refers to the network of interconnected devices embedded with sensors, software, and connectivity capabilities, enabling them to collect and exchange data. These devices may include objects like smartphones and wearables to specialized sensors and actuators. With respect to the retail industry, IoT holds tremendous promise in improving operational efficiency with optimizing supply chains, and delivering incomparable customer experiences. IoT empowers retailers to gather real-time data, gain valuable insights, and make data-driven decisions by connecting physical objects and integrating them into digital ecosystems.

In retail, IoT applications incorporate various areas such as personalized marketing, inventory management, smart checkout systems, customer engagement, and optimization of store operations. For example, IoT devices can track inventory levels at stores as well as at warehouses and can send updates to concern departments, monitor product conditions, and also trigger reordering processes automatically. Similarly, for customers, IoT-powered beacons and sensors can facilitate personalized offers and promotions, effectively guiding customers through the shopping journey. Technologically extended smart shelves and digital signage can offer interactive and engaging product displays (Vass, 2020). Moreover, IoT can empower retailers to leverage data analytics, can perform predictive algorithms, and machine learning to better understand consumer habits and preferences, anticipate consumer demand, and elevate inventory levels (Felipe Caro, 2019). IoT enables seamless Omni channel experiences, assisting customers to switch between online and offline channels without disruptions.

(Obaidat and Obeidat, 2020). Although IoT offers enormous opportunities to customers and retailers, it also presents some significant challenges which include data security and privacy concerns, interoperability issues, and need for robust infrastructure. Conversely, retail industry continues to evolve, embracing IoT

technologies has become imperative for retailers to stay competitive, meet customer expectations, and create differentiated experiences.

5.4 Overview of the Importance of Customer Experience in the Retail Industry

(Dr. Shrikant Waghulkar, 2018) In recent years, retail industry has undergone a significant shift with customer experience which is emerging as a crucial factor for their success. Customer experience refers to the overall interaction and perception that customers have while engaging with a retailer or brand . It incorporates every touchpoint, from the moment customers ascertain a product or service to the post-purchase support they receive. In today's competitive environment, where consumers have ample choices and alternatives with high expectations from product/service, delivering extraordinary customer experiences has become challenging for retailers (Jabil, 2023). Customer experience is the key to retail success in a market overrun with limitless product possibilities. However, it is easier said than done to provide a memorable and consistent retail consumer experience in an omni-channel environment. New expectations have emerged in the transactional interaction between retailers and their customers. (V Kumar, 2016) The seamless integration of physical and digital experiences, achievement of operational efficiency, and effective use of data to produce actionable customer insights are all requirements. An appropriate customer experience can offers substantial advantages like increased customer satisfaction and loyalty, differentiation from competitors, positive brand perception and reputation, word-of-mouth marketing, improved customer retention and lifetime value, personalized engagement, emotional connections, increased level of profitability, reduced customer churn, quality data insights for continuous improvement, customer-centric culture, alignment with sustainability and ethical values and many more such trends are been seen and observed.

5.5 Role of IoT in Transforming and Personalizing Customer Experiences

(Keough, 2023) IoT had played pivotal role in transforming and personalizing customer experiences by enabling retailers to proactively address customer needs by predicting maintenance issues or replenishment requirements of customer purchases). Enterprise leaders can incorporate a proactive CX framework that modifies operations to deliver customer happiness using IoT-enabled connectivity. As per studies, two-thirds of brand loyalty is driven by CX. Operations are shaped by IoT integration to prioritize client pleasure. The ability to deliver personalized

experiences not only fosters customer satisfaction and loyalty but also provides retailers with a competitive edge in the dynamic marketplace. Through IoT-powered solutions, retailers can create a more connected, customized and convenient shopping experience which meets the unique preferences and personalized demand of customers. Ultimately, IoT empowers retailers to transform customer experiences, delivering a new level of personalization, convenience and ultimately leading towards a satisfied customer. Additionally, IoT enables retailers to gain a better understanding of customer behaviour and preferences by collecting and analysing data from different point of contact. This data-driven approach allows retailers to anticipate customer needs and proactively offer relevant set of products or services. By leveraging IoT analytics, retailers can discover buying patterns and trends of the customers that helps to upgrade their marketing strategies, optimize inventory management, and streamline operational processes at their stores. Besides, IoT also facilitates real-time communication between customers and retailers allowing exchange of instant feedback, personalized support, and effective issue resolution. Through smart home devices, mobile applications, and voice assistants, customers can interact seamlessly with retailers, making inquiries, placing orders, or accessing personalized recommendations. This unified integration of IoT into the customer experience creates a more convenient, efficient, and personalized journey for customers, ultimately strengthening their loyalty and affinity towards the brand. Overall, the role of IoT in transforming and personalizing customer experiences is significant, empowering retailers to deliver exceptional service, drive customer satisfaction and survive in the digital era.

5.6 Understanding Customer Expectations in the Digital Age

(Maria Holmlund, 2020) In this digital age, understanding customer expectations is important for businesses to prosper in a highly competitive market). Customer experience (CX) has become an effective means of differentiating businesses in the market. Big data analytics (BDA) has recently made advancements that have revealed opportunities to extract customer insights for CXM. Today customers have higher expectations and are empowered than ever before as they demand seamless experiences across various channels which includes both online and offline. Businesses must ensure consistency in branding, frequent reminder through various marketing communications and overall customer data tracking in order to provide a cohesive experience. In this highly competitive era personalization has become a key driver of customer satisfaction. Customers expect businesses to understand their preferences and needs, and give them recommendations of offers, and content accordingly. By leveraging customer data and advanced analytics, businesses can alter their offerings to individual customers,

creating a more personalized experience that reverberates with their interests. This opportunity of personalization can lead to Customer Lifetime Value (CLV). In today's digital age, consumers expect mobile-friendly experiences, where websites, mobile applications, and various interfaces are optimized for seamless use on their smartphones. Customers also value instantaneous access to accurate information like product details, its availability, pricing, and customer support. Quick response times, efficient service, and prompt issue resolution are crucial in providing a frictionless customer experience.

Furthermore, the rise of social media has transformed customer interactions, with customers expecting businesses to actively engage with them on these platforms, respond to their queries, and address their concerns round the clock. Data security and privacy have become utmost concerns, and customers expect businesses to prioritize the protection of their personal information through transparent data collection practices, robust security measures, and compliance with data protection regulations. Moreover, while doing digital payment, seamless payment experiences are expected, with consumers looking out for secure payment mechanisms, such as integrating various payment gateways and enabling contactless payments. Finally, customers appreciate payment houses that focus on continuous improvement and round the clock innovation based on the feedback and suggestions received along with keeping a track of changing needs of customers. By embracing customer-centric approaches, leveraging technology, and analyzing customer data, businesses can exceed customer expectations and forge meaningful connections in the digital age.

5.7 The Demand for Personalized and Seamless Shopping Experiences

(Erik Lindecrantz M. T., Lindecrantz, 2021) The rise of e-commerce pioneers like Amazon has led customers to expect and demand personalized experiences. According to a research conducted by Epsilon and GBH Insights revealed that a significant majority (80%) of US adults desire personalization from retailers. Personalization has become a hygiene factor, where customers consider it a basic expectation, and if a retailer fails to deliver, customers may switch to a competitor. The concept of personalization has expanded beyond targeted offers and now encompasses the entire customer experience. Customers now seek personalization across various touchpoints, allowing them to allocate their time and money based on their preferences. In the best personalized experiences, retailers engage customers in a dialogue and utilize data to create one-to-one personalization rather than generic segment-level offers, customers receive targeted offers, products, and communications that sounds relevant for them as an individual.

5.8 Understanding How Personalization Pays Off

In order to stand out and survive, in today's competitive landscape, retailers must not only meet but exceed customer expectations for personalized experiences. When implemented effectively, personalization goes beyond survival and empowers retailers to thrive. Implementing personalized experiences at scale can lead to a significant increase in total sales, with grocery companies experiencing 1 to 2% lift and other retailers achieving even higher boost in loyalty and share-of-wallet among already-loyal customers. (Erik Lindecrantz M. T., Lindecrantz, 2021) Additionally, such programs can result in cost savings of around 20% in marketing and sales. Successful personalization initiatives not only drive revenue growth but also foster more engaged customers. A positive customer experience leads to more than 20% higher customer satisfaction rates, almost 15% increase in sales conversion rates, and about 30% rise in employee engagement. Retailers who consistently deliver exceptional customer experiences have achieved three times higher returns for their shareholders compared to those with lower customer satisfaction scores. To optimize the outcomes of personalization programs, it is recommended to initially focus on the most loyal customers, as targeting regular shoppers yields a significantly higher return on investment compared to mass promotions. Moreover, prioritizing data collection on loyal customers creates a virtuous cycle, generating increasingly relevant data and higher response rates, ultimately enhancing the overall quality of customer data (Erik Lindecrantz, 2021).

As the customer journey continues to evolve, encompassing a wide array of channels such as social media, newsletters, online stores, and customer service support, maintaining a seamless and consistent experience has become paramount (Howell, 2018). This holds true especially for retailers operating both online and brick-and-mortar locations, where aligning the customer experience across all touchpoints is essential for establishing credibility. In the modern landscape, customers expect every interaction with a brand to be connected, relevant, and convenient. For instance:

- 75% of consumers anticipate a consistent experience, regardless of the engagement channel they choose, be it a website, social media, mobile device, or in-person encounter.
- 64% of consumers seek personalized offers tailored to their preferences from retail brands.
- 56% of consumers are willing to share their data in exchange for faster and more convenient service.

To meet these evolving expectations, businesses must focus on seamlessly integrating their various channels and providing a unified experience. By delivering consistency, personalization, and convenience, retailers can forge stronger connections, boost customer satisfaction, and cultivate lasting loyalty in today's dynamic and competitive marketplace.

Companies in the retail and hospitality sectors should concentrate their efforts on three key areas to handle this significant shift in behaviour. The areas are as follows:

1. **Omni Channel Experiences:** By 2025, it is anticipated that the worldwide e-commerce market would be worth \$7.4 trillion. The growing emphasis on omni channel experiences, where brands provide customers with a variety of experience alternatives, encompassing both physical locations and digital channels, is one of the major growth drivers in this market. This practice has spread over a variety of sectors, including gaming and retail, illustrating the universal expectations customers have for frictionless interactions with firms. Companies that execute this strategy effectively generate frictionless (and frequently personalized) brand experiences that encourage favourable encounters both online and offline.

In order to successfully stand out of the crowd, changing landscape, businesses must consider their role in the expanding Omni channel ecosystem. If consumer profiles are not compatible, keeping an e-commerce site and a few brick-and-mortar shops is insufficient.

2. **Immersive Experiences and AR:** Companies were unable to rely on their major, legacy channels when the pandemic prompted many physical sites to close for extended periods of time. While “try-before-you-buy” experiences were popular in the retail industry, for instance, they needed to be rethought once stores reopened and customers searched for an equivalent experience. According to research done by my own business, cosmetic businesses have embraced this new field by implementing augmented reality (AR) to give customers a safer alternative to assist them in finding the best foundation shade for their skin tone.

In the new normal, consumers’ interactions with companies will continue to be heavily influenced by their worries about health and safety. Contactless communication gaps between businesses and their customers will be bridged by immersive AR and VR technologies.

3. **Hyper-personalization:** In order to create innovative client experiences, technology is a crucial element. This includes the capability to personalize, or deliver customized messaging and offers to customers at particular touchpoints along their journey. The societal determinants, market trends, and even order history are some of the more conventional factors that customization is driven by.

Hyper-personalization, enabled by recent developments in artificial intelligence (AI), is raising the bar for this trend. The potential of this strategy is far greater and covers a wide range of additional topics, including content generation, suggestions, media mix, omni channel, customer experience, and others. A brand experience that is even more seamless and that knows the customer better than ever may be created by using behavioural data to give pertinent promotions and customized communications in real time. The data

may also be utilized to assist the company develop its content strategy and also work on increasing their social influence.

5.9 IoT-enabled Personalization and Customization

Personalization and customization is made possible by IoT in the retail sector. It has further revolutionized how companies meet the needs of each unique client. Businesses can gain insightful information about the preferences and behaviour of their customers through real-time data collecting. These data allow companies to create tailored product setups, modify user interfaces, and make personalized product suggestions. Along with voice-activated personalization and better supply chain visibility, IoT devices enable proactive service and support, predictive maintenance, location-based personalization, dynamic pricing and offers. In general, IoT technology equips companies to provide seamless and highly personalized experiences that raise client engagement and happiness.

5.10 Leveraging IoT Data for Personalized Product Recommendations

In today's cutthroat retail environment, using IoT data for personalized product suggestions has changed the game for businesses. Businesses may improve customer engagement, spur revenue development, and cultivate long-term customer loyalty by utilizing real-time data, applying advanced analytics and machine learning, and providing highly contextualized recommendations. Businesses must invest in IoT data analytics capabilities to stay ahead in the rapidly changing retail industry as IoT technology develops and more data is created, creating more opportunity for businesses to deliver personalized experiences.

One of the primary areas where the IoT plays a critical role is in making personalized product suggestions. In today's digital age, businesses aim to provide their customers with personalized experiences. IoT devices provide enormous amounts of data from linked sensors and gadgets, giving businesses insightful knowledge into the preferences and behaviours of specific customers. By utilizing this vast amount of IoT data, companies may provide highly individualized and pertinent product recommendations, boosting the overall customer experience and promoting customer happiness and loyalty in some of the following ways:

1. Harnessing Real-Time Data:

Real-time data is gathered by IoT devices on a variety of client interactions, including browsing history, purchasing trends, product usage, and location. As a result, firms are able to provide customized product recommendations by better understanding client preferences and behaviours. Businesses may provide

precise and timely recommendations that address the specific needs of customers by analyzing real-time data to find patterns, correlations, and trends.

2. Advanced Analytics and Machine Learning:

Businesses use advanced analytics and machine learning techniques to glean valuable insights from the massive volumes of IoT data. Algorithms for machine learning may analyze client data, spot trends, and produce tailored suggestions based on distinct interests and behaviours. These algorithms continuously adapt and learn, improving their ideas over time to provide ever-more-accurate and pertinent advice.

3. Contextualized Recommendations:

Using IoT data, organizations may provide highly contextualized suggestions by taking into account a range of variables including client demographics, purchasing behaviour, browsing habits, and geography. For instance, a retail establishment using IoT sensors can identify a customer's presence in a certain aisle and suggest appropriate products based on that customer's position. With this level of contextualization, recommendations are guaranteed to be pertinent, timely, and in line with the client's current requirements.

4. Enhanced Customer Engagement:

IoT-based personalized product recommendations increase client engagement by making suggestions that are pertinent to them. Recommendations that fit the preferences of the client are more likely to be acted upon, improving the likelihood of conversion and customer satisfaction. Additionally, personalized recommendations develop a feeling of individual attention, which makes clients feel appreciated and thereby help in strengthening client relationships.

5. Cross-Selling and Upselling Opportunities:

By examining client purchasing trends and preferences, firms are able to find cross-selling and upselling prospects using IoT data. Businesses can increase the average order value and spur revenue growth by recommending upgraded products or complementary items by analyzing the connection between various products and client preferences.

6. Improving Customer Retention:

IoT data-driven personalized product recommendations aid in efforts to keep customers. Customers are more likely to make additional purchases from a firm when they are given recommendations that are suited to their interests and preferences. This customized strategy distinguishes firms from their rivals by fostering consumer loyalty and a positive brand perception.

7. Continuous Improvement and Adaptation:

Businesses can track the success of their ideas and alter them as necessary by continuously monitoring IoT data. Businesses may improve the accuracy and relevance of future suggestions by fine-tuning their recommendation algorithms and tracking client replies, comments, and purchasing patterns. The personalized product recommendations will continue to be useful and beneficial for clients over time thanks to the streamlined process.

8. Personalizing shopping experience based on customer preferences:

Personalized online shopping experiences helps the clients engage with your brand that are specific to their preferences or profile. This may be a suggestion tool using AI that learns from user behaviour. Alternatively, it might be a self-directed returns portal with free shipping labels and real-time tracking data. Every stage of the client journey can be customized, from the initial visit through after the transaction.

The basics of retail have been transformed by ecommerce and online shopping, but also consumer behaviour. Customers nowadays are highly developed, educated, and hold themselves to very high expectations. In addition, there is a plentiful supply, so if a brand does not satisfy customers' needs, they will locate another one that does (Erik Lindecrantz, 2020). Customers favour brands that use their offers and marketing to create a personalized buying experience, according to 75% of consumers. Customers also consent to having their mobile apps track their activities in order to receive interest-specific, tailored adverts.

5.11 Personalized Shopping Experience

In the words of McKinsey (Clootrack, 2022), “Personalization, once limited mainly to targeted offers, now extends to the entire customer experience. This means that customers want personalization throughout their interactions with a retailer—with multiple, personalized touchpoints that enable them to allocate their time and money according to their preferences.” Personalizing the customer experience is making it more suited to each individual's demands. Remembering the customer's name or developing a new product just for them are examples of personalization. Because it bases itself on an emotional bond between a company and the customer, customer engagement thrives on a personalized purchasing experience. Brands may personalize how they interact with and market to their customers, from straightforward activities to intricate data-driven customer engagement tactics.

In order to appeal to each consumer's unique tastes and preferences, any campaign, product, or service must be meticulously designed. Targeted dynamic scenarios, product recommendations, and exclusive discounts result from data collection based on prior behaviour or segmentation of the population. The full customer journey is what ecommerce personalization refers to, it should be present in every brand-consumer interaction, and it necessitates commitment to the goal.

5.12 Importance of Personalized Shopping Experience

In essence, conversions and growth are ultimately the reasons why each company should concentrate on offering the greatest personalized shopping experience



Figure 5.1 Importance of personalized customer experience.

Source: https://clootrack.com/knowledge_base/customer-experience-personalization

(Ledesma, 2021). According to surveys, organizations who excel at customer experience get an average 17% increase in revenue, compared to businesses that fall short by only 3%.

Brands that do this well enjoy a significant increase in consumer loyalty and average savings of 10–20% on marketing expenses overall. Personalization is effective because it demonstrates to customers that a brand values their business and is concerned with their unique demands. In the long run, this helps brands increase their CLV (Customer Lifetime Value); the personalized approach strengthens the brand-customer relationship and encourages loyalty based on symbolic or material benefits. Companies should build personalization strategies so as to lure customers towards them continuously. Some of the reasons why personalized shopping experience becomes necessary are enumerated in (Figure 5.1) and the description is as under:

1. **Increases loyalty:** Customers are more likely to return to the same business when they feel appreciated and well-treated. If they have a positive encounter with a brand, they might even tell their friends and relatives about it. Customers are not only retained, but the consumer base is also expanded as a result.
2. **Improves the rate of customer retention:** 44% of shoppers will return to a company if they had a personalized purchasing experience with their prior purchase, according to the Segment's Personalization Report. Conversely, 70% of buyers claimed they are dissatisfied with firms who refuse to give customized shopping experiences.
3. **Recognize client expectations:** Customers want brand house to take extra and unexpected activities across all touchpoints they interact with, in

addition to the quality of the items they buy. For instance, a lot of buyers anticipate that salespeople in-store will be aware of their prior online interactions with the business.

4. **Provides Firms with A Competitive Edge:** A company differentiates itself from its rivals by providing a personalized customer experience. Every business needs a distinct quality or trait that sets it apart from the other competitors in the market. Businesses can gain an advantage over rivals in the market by offering distinctive customer-centric techniques like individualized chat assistance and email help.
5. **Improved client satisfaction:** Customers will without a doubt be entirely satisfied with a brand if they feel they receive what they need according to their tastes and preferences.
6. **Increased Effectiveness:** Businesses may employ cutting-edge tools to offer each consumer a distinctive experience because they have access to customer information at their fingertips. Personalization speeds up problem solving since businesses already know all there is to know about the client.
7. **An Increase in Order Volume:** Customers will buy more things from a store they weren't going to when they entered if they had a personalized shopping experience. Additionally, if customers experience a personalized setting in a store, they are more likely to purchase more expensive goods.
8. **Product Returns Are Lessened:** A consumer is more likely to be happy and utterly satisfied with their purchase and products when they receive a personalized experience. This suggests a lower likelihood of product returns.

5.13 Examples of Personalized Customer Experience

Brands have redefined the customer experience over the past couple of decades, as we have seen. They have established a high standard and carved out a distinctive name for themselves in the marketplace (Cornell, 2022). Let's look at a few well-known brands that have mastered personalization:

■ **Amazon Recommends the Products You Really Need**

The world's largest online retailer, Amazon, has established the benchmark for all other companies when it comes to personalized suggestions. We have all encountered websites that propose things when we are shopping online. Millions of Amazon consumers worldwide get personalized homepages thanks to AI technology. In addition, Amazon's algorithm takes in to consideration purchasing pattern of consumers their past purchases, and a number of other aspects like Demographics to suggest products as per their browsing and search history.

■ **Nike Brings Out the Designer in You**

Nike's well-known customization campaign "Nike By You", lets customers customize their Nike footwear, has garnered attention on a global scale. Customers can utilize various materials, colours, and other designer elements while letting their creativity run wild.

Now, many would question why a billion-dollar company like Nike would need to customize things when it could offer particular designs with ease. The explanation is rather straightforward: by letting customers customize their sneakers, Nike gives them the freedom to show their uniqueness.

■ **Stitch Fix Delivers 'Tailor-Made' Customer Experiences**

Stitch Fix is much more than your typical online fashion retailer. It is a U.S.-based online personal style company that customizes clothing for customers—men, women, and children—using sophisticated algorithms and data science. Customers are required to provide measurements and pass an obligatory style test. Then, a Stitch Fix stylist purchases 5 pieces of clothes to match the person's own style and ships them. Customers can retain or return products they receive, which helps the recommendations get better over time.

■ **Apple's shopping experience**

Apple have spent years building a distinctive brand that values their clients. Enter any of their stores, and their support team will be there to assist you with any issues you might be having in addition to helping you buy things. They provide customer support for the duration of a product's life.

5.14 Smart Retail Environments

Intelligent and networked retail spaces are referred to as "smart retail environments" (SREs). These SREs use a variety of digital technologies, such as the IoT, Artificial Intelligence (AI), data analytics, and automation, to optimize and improve the shopping experience for customers. To enable real-time data gathering, analysis, and automation in order to enhance shop operations, boost consumer engagement, and promote corporate success, these settings integrate smart devices, sensors, and data analytics systems. It improves store operations and the shopping experience for customers. It has a number of advantages, including improved output sustainability, quality, and efficiency. Although the lack of technology adoption in the unorganized retail sector restrains the growth of this market, the rising cases of shoplifting and the increasing adoption of disruptive technologies to forecast future market trends are expected to create growth opportunities for the stakeholders in this market (Alexander Volz, 2021). For example, since the emergence of e-commerce, physical retail has encountered several difficulties. Its destruction has been predicted more and more frequently in recent years. Since 2001, the literature has used the word "retail apocalypse" to refer to the rapidly increasing demise of brick-and-mortar businesses in the United States.

The growth of the smart retail market is driven by the growing need to improve customer experiences and retail operations as well as the increasing number of smart stores. Multiple interconnected parts come together to form an intelligent ecosystem in a smart retail setting. This comprises IoT gadgets that gather information on customer behaviour, inventory levels, and store conditions, such as sensors, beacons, and RFID tags. Advanced analytics and AI algorithms are then used to process and analyze the obtained data in order to produce insights that can be used to make decisions (Eleonora Pantano, 2014). The extensive usage of sophisticated systems raise fresh concerns about the wise application of technology. In fact, effective technology utilization can be considered as an organizational challenge and as a force that transforms conventional buying and selling practices. The use of modern technologies is particularly a component of a movement towards the building smart cities to improve urban life as well.

Customers are empowered by smart technology in two ways during the purchasing process in smart retail establishments (Jiahe Chen, 2023). First, the distinctive value that smart technology offers is demonstrated by the higher level of convenience and second the lower level of social presence. Smart retail, by definition, produces a sales process that is decentralized, transparent, and optimized for both the store and the larger supplier chain. Beyond the general features, several businesses instead place an emphasis on specific advantages. To that end, the advantages of smart retail include improved output sustainability, quality, and efficiency, we can narrate them as under:

1. **Efficiency:** The most advantageous aspect of smart retail is self-adaptation and how it affects efficiency. Smart retail will analyze and self-correct to make the sales and adaption process, as well as its output, as efficient as possible when fully operational, efficient algorithms have constant access to an ever-changing stream of data.
2. **Quality:** Smart retail's result never has a chance to suffer because of its capacity to identify and fix possible problems before they have a chance to become seriously troublesome. Because non-smart methods occasionally yield subpar outcomes, the quality of any smart retailer's output will tend to be higher than any of those produced by non-smart means.
3. **Sustainable Output:** Disruptions have been known to occur occasionally in traditional retail and sales environments, whether they are brought on by labour, environmental, or unintentional circumstances. The danger of human error is eliminated by the adaptability and self-correction mechanisms offered by smart retail. Therefore, its automation can lead to improved output sustainability and increased safety.
4. **Upgradation of Workforce Skills:** Such a transformation in an industry's procedures cannot occur without having some effect on the typical worker. The function of the human work has altered, much like in previous

industrial revolutions. A technical skill set will be required as people transition away from manual labour and towards technological support.

5.15 Smart Shelves and Digital Signage for Interactive and Engaging Displays

Two essential elements of a smart retail environment that improve customer interaction and offer interactive and interesting displays are smart shelves and digital signage. Nearly every aspect of our lives has been touched by technology, and the retail industry is no exception. Whether it's self-checkouts, online storefronts, or ecommerce, technology has sparked a revolution. The impact of technology on retail, particularly on shelves, cannot, however, be ignored. If there was ever a truly remarkable invention, smart shelves are among the best. Retailers today employ a variety of techniques to improve the in-store shopping experience.

5.15.1 Smart Shelves

IoT sensors and other technology are used in smart shelves to deliver real-time data on product availability, cost, and other pertinent information. Retailers can precisely maintain inventory levels and speed restocking procedures thanks to these shelves' ability to identify when an item is removed from or returned. Additionally, dynamic pricing, promotions, and product information can be displayed on smart shelves to create an engaging and visually appealing shopping experience. Customers may quickly access product information, evaluate prices, and decide on a purchase with knowledge. Additionally, customers may explore more product details, read reviews, or even place orders directly from the shelf by integrating smart shelves with touchscreen interfaces or mobile apps.

5.15.2 Digital Signage

Digital signage is the use of digital displays, such as LCD screens, LED panels, or interactive kiosks, to present clients with relevant and interesting material. These displays can be put in key locations throughout the store to draw attention from customers and deliver marketing messages, product details, or customized offers. Retailers can dynamically change content on digital signage based on customer demographics, the time of day, or other contextual considerations. For instance, a digital sign by the entry could greet customers and advertise current sales, while displays in certain product sections might feature pertinent product films or client endorsements. Customers can interact with the content of interactive digital signage by using touchscreens to choose product options or access further information.

5.16 Some of the Benefits of Smart Shelves and Digital Signage

Enhanced Customer Experience: Interactive and aesthetically pleasing shopping experiences are provided by smart shelves and digital signs, enabling customers to obtain product information, weigh their options, and make wise decisions. Increased consumer involvement and satisfaction result from this.

Real-Time Updates: Time-sensitive information, promotions, or price changes can be instantaneously communicated by merchants using both smart shelves and digital signage that can be updated in real-time. Customers will always have access to the most recent information thanks to this.

Personalization: Depending on the preferences, past purchases, or position of the customer within the store, digital signage can be tailored to display specific material. This personalization contributes to making the buying experience more pertinent and interesting.

Effective Inventory Management: Retailers may monitor product availability and automate inventory management procedures using smart shelves with IoT sensors. This prevents out-of-stock situations by making sure that shelves are appropriately filled.

Opportunities for Marketing and Promotion: Digital signage offers a platform for showcasing sales, new items, or cross-selling possibilities. These displays can help retailers enhance sales, brand loyalty, and customer awareness.

Data Gathering and Analytics: Digital signs and smart shelves produce useful information on customer interactions, such as preferences for products and levels of engagement. These data can be analyzed by retailers to better understand consumer behaviour, improve marketing plans, and make data-driven business decisions.

Businesses may build interactive and compelling displays that improve the entire customer experience, increase operational efficiency, and boost sales by integrating smart shelves and digital signage into a retail setting.

5.17 Real Time Inventory Management System and Product Availability

IoT sensors are essential for the retail sector's real-time inventory tracking and product availability. These sensors provide precise and current information on inventory levels, product movements, and availability by utilizing cutting-edge technology including RFID, barcode scanning, weight and pressure sensing, ambient monitoring, motion and proximity sensing, and sensor fusion techniques.

Wireless transmission of the data gathered by these sensors to a central database or cloud-based platform enables real-time access to inventory data. Retailers can use this information to track product availability, automate inventory management

procedures, and make informed decisions. Additionally, IoT sensors can be used with predictive analytics, machine learning, and AI algorithms to better decision-making, optimize inventory levels, and forecast demand.

The functionality and dependability of IoT sensor systems are further improved by sophisticated features including advanced localization, cloud-based platforms, data security measures, integration with ERP systems, and real-time notifications. These capabilities help businesses create a greater customer experience, accomplish seamless inventory management, increase operational efficiency, and decrease stock outs (Sheakh, 2018). Increased sales and profitability, a better work environment, and an overall rise in customer satisfaction are all examples of how inventory management will pay for itself.

Additionally, organizations can avoid the complexity of manual processes and keep track of stocks in real-time with the help of IoT and RFID (Vidushi, 2022):

1. **Instantaneous input for effective supply chains:** Several technologies are used by IoT devices to facilitate touchless data collection. IoT devices use GPS and other technologies to track and verify packages and shipments, including Radio Frequency ID (RFID) chips, smart devices, and mobile sensors. Blume Global claims that the enormous amount of data that is currently accessible through IoT devices, wearables, and merchants enables real-time inventory visibility.
2. **Management Storage:** Improvements in 5G wireless technology and the application of IoT-enabled devices are helping to improve warehouse management logistics. The goal of warehouse management is to make the best possible use of available space. If the utilization pattern is known, the space that is available in a warehouse may be better allocated. More frequently used items may be kept nearer the entry points in the warehouse to improve efficiency.
3. **Algorithms for artificial intelligence:** We now have the ability to develop intelligent algorithms that can track and manage inventory far more effectively than a human could. By carefully examining IoT data, AI technologies will help in identifying trends that humans are unable to perceive. Undoubtedly, this process will improve decision-making in inventory management. Systems for managing inventory that use AI are better able to handle tasks like ordering replacement inventory.
4. **IoT delivers improved inventory tracking and precise location monitoring:** According to The Daily Plan IoT, products marked with IoT devices help with more effective storage and distribution. The location and timing of product delays in transit may be identified utilizing inventory tracking and route planning using IoT devices. This aids in planning for emergencies and finding faster supply chain alternatives.
5. **Improved Lead Management:** IoT-based inventory tracking is critical in estimating the lead times required to assemble all the parts required for production. High lead times are identified in order to minimize stumbling

blocks caused by a vital part(s) being absent and causing manufacturing process stoppages. This improves the synchronization of manufacturing operations and inventory demand fulfilment. As a result, manufacturing processes and inventory demand fulfilment are better coordinated.

5.18 Conclusion

In conclusion, the introduction of IoT technology has sparked a tremendous change in the retail sector and raised the quality of the customer experience to entirely new levels. Businesses now have the ability to collect and analyze enormous volumes of real-time data, empowering them to make better decisions and provide more individualized experiences to their customers. This is made possible by the integration of IoT applications into many elements of retail operations.

However, while the potential of IoT in retail is immense, it is essential for businesses to prioritize data security and privacy. With the increased connectivity and data exchange involved, robust security measures must be implemented to safeguard customer information and protect against potential cyber threats. IoT application integration in the retail industry has sparked a surge of innovation and changed how companies engage with customers. Retailers can personalize experiences, streamline operations, and ultimately increase consumer happiness by utilizing the power of IoT devices and data analytics. In future, the shopping experiences will be increasingly more immersive and linked thanks to IoT technology's continued development and growth in impact on the retail sector will continue to advance even further.

References

- Alexander Volz, P. H. (2021). *Smart Retailing Technologies to Counter Current Retail Challenges - An Assessment of Impacts*. The 23rd International Conference on Information Integration and Web Intelligence. 10.1145/3487664.3487808
- Clark, B. (2021, August 27). 7 Technological Advancements in the Retail Industry to Make You Say Wow. *7 Technological Advancements in the Retail Industry to Make You Say Wow*. Acquire. Retrieved June 2023, from <https://acquire.io/blog/technological-advancements-retail-industry>
- Clootrack. (2022). *What is Customer Experience Personalization?* Retrieved June 14, 2023, from https://www.clootrack.com/knowledge_base/customer-experience-personalization
- Cornell, J. (2022, December 06). *Personalized Customer Experience: What, How, and Why*. Retrieved from ProProfs Help Desk: <https://www.proprofsdesk.com/blog/personalized-customer-experience/>
- Dr. Shrikant Waghulkar, D. N. (2018). *A Theoretical Perspective on Customer Experience (CX) in Digital Business Strategy*. Amravati: IEEE. 978-1-5386-2599-6/18/\$31.00
- Eleonora Pantano, H. T. (2014, December 6). What is smart for retailing? *Procedia Environmental Sciences*, 22, 101–107. Retrieved from <https://www.sciencedirect.com/science/article/pii/S1878029614001571>

- Erik Lindecrantz, M. T. (2020). *Personalizing the Customer Experience: Driving Differentiation in Retail*. Retrieved June 13, 2023, from <https://www.mckinsey.com/industries/retail/our-insights/personalizing-the-customer-experience-driving-differentiation-in-retail>
- Erik Lindecrantz, M. T. (2021). *Personalizing the Customer Experience: Driving Differentiation in Retail*. Retrieved April 22, 2023, from <https://www.mckinsey.com/industries/retail/our-insights/personalizing-the-customer-experience-driving-differentiation-in-retail>
- Felipe Caro, R. S. (2019). The Internet of Things (IoT) in retail: Bridging supply and demand. *Business Horizons*, 62(1), 47–54. 10.1016/j.bushor.2018.08.
- Forbs (2021, Oct 14). *Leveraging IoT Solutions to Improve Customer Experience*. Retrieved April 2023, 22, from IoT2Market: <https://iot2market.com/newsView/leveraging-iot-solutions-to-improve-customer-experience>
- Gupta, D. G. (n.d.). Retrieved from Academia: https://www.academia.edu/9114417/Retail_industry_research_paper
- Howell, L. (2018). *Customer Experience and Design-The Need for a Seamless Shopping Experience*. Retrieved April 23, 2023, from <https://blogs.perficient.com/2018/04/10/seamless-shopping-experience/>
- Jabil. (2023). *What's in Store for Rethinking Retail? Customer Experience*. Retrieved from Jabil: <https://www.jabil.com/blog/retail-customer-experience.html>
- Jiahe Chen, Y.-W. C. (2023, April 3). How smart technology empowers consumers in smart retail stores? The perspective of technology readiness and situational factors. *Springer Link*, 33(1), 1–24. 10.1007/s12525-023-00635-6
- Keough, D. (2023, June 2). *Meeting Evolving Customer Demands With IoT-Enabled Connectivity*. Retrieved from CMSWIRE: <https://www.cmswire.com/customer-experience/meeting-evolving-customer-demands-with-iot-enabled-connectivity/>
- Ledesma, J. (2021, November 17). *Why Personalized Experiences can Boost Conversions*. Retrieved June 12, 2023, from Trustpilot: <https://business.trustpilot.com/reviews/brow-sers-to-buyers/why-a-personalized-consumer-experience-matters-in-the-ecommerce-world>
- Leszek Marek, J. W. (2017). The Internet of Things as a customer experience. *Jagiellonian Journal of Management*, 3, 163–176. 10.4467/2450114XJJM.17.011.9562
- Maria Holmlund, Y. V. (2020, August). Customer experience management in the age of big data analytics: A strategic framework. *Journal of Business Research*, 116, 356–365. 10.1016/j.jbusres.2020.01.022.
- Obaidat, M. A., and Obeidat, S. (2020, May 30). A comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, 9(2). 10.3390/computers9020044.
- Pan Wang, R. V. (2015, April). Introduction: Advances in IoT research and applications. *Information Systems Frontier*, 17(2). 10.1007/s10796-015-9549-2.
- Pradyumna Gokhale, O. B. (2018, January). Introduction to IOT. *International Advanced Research Journal in Science, Engineering and Technology*, 5(1), 41–44. 10.17148/IARJSET.2018.517.
- Sheakh, T. (2018, May). A study of inventory management system case study. *Journal of Dynamical and Control Systems*, 10, 1176–1190. Retrieved June 16, 2023, from https://www.researchgate.net/publication/327793184_A_Study_of_Inventory_Management_System_Case_Study#fullTextFileContent

- Shotwell, L. (2022). *7 Retail Technology Innovations Reviving the Stores in 2023*. mobidev. Retrieved 2023, from <https://mobidev.biz/blog/7-technology-trends-to-change-retail-industry>
- V Kumar, W. R. (2016). Creating enduring customer value. *Journal of Marketing*, 80(6), 36–687. 10.1509/jm.15.0414.
- Vass, T. A. (2020, June). IoT in supply chain management: A narrative on retail sector sustainability. *International Journal of Logistics Research and Applications*, 24, 1–20. 10.1080/13675567.2020.1787970.
- Vidushi. (2022, March 1). *IoT in Inventory Management and Tracking*. Retrieved from psiborg: <https://psiborg.in/iot-in-inventory-management-and-tracking/>
- Wayne D. Hoyer, M. K. (2022, January 31). Transforming the customer experience through new technologies. *American Marketing Association*, 51(1), 57–71. 10.1016/j.intmar.2020.04.001.

Chapter 6

Healthier Horizons: Exploring IoT's Impact on Education and Well-Being

Mohammad Amin Dar¹, Insha Rasool¹, and
Faheem Syeed Masoodi²

¹*Department of Education, University of Kashmir, Srinagar, Jammu and Kashmir, India*

²*Department of Computer Science, University of Kashmir, Srinagar, Jammu and Kashmir, India*

6.1 Introduction

The integration of Internet of Things (IoT) technologies in various domains has transformed the way we live, work and interacts. In the realm of education, IoT offers new opportunities to create innovative and immersive learning environments that can be tailored to individual needs, facilitate personalized learning experiences and provide real-time data to inform instructional strategies. Moreover, IoT has the potential to extend beyond the classroom, contributing to students' overall well-being by promoting healthy habits, enhancing safety measures and enabling remote access to educational resources. This chapter aims to explore the wide-ranging influence of IoT on learning and health, encompassing not only academic outcomes but also the holistic development of students. The main argument or claim of this chapter is that IoT can create healthier horizons in education by enhancing students' academic performance, physical health, mental health, social

skills, creativity, digital literacy and career readiness. However, this potential can only be realized if educators, policymakers and researchers collaborate to address the challenges and ethical issues associated with IoT in education. Therefore, this chapter seeks to provide a comprehensive overview of the current state of knowledge on IoT in education and its effects on well-being. It also aims to identify gaps in the literature and offer recommendations for future research directions in this field.

The chapter is structured as follows: first, we provide a literature review on four main themes related to IoT in education: (1) the use of IoT devices in early childhood education; (2) the use of IoT devices in higher education; (3) the impact of IoT technology on education in 2023; and (4) the role of IoT in education. We summarize each theme and provide a critical analysis of the existing studies. Second, we explore how IoT devices can enhance academic outcomes in education by discussing the role of personalized learning experiences, real-time data analysis and instructional strategies informed by IoT-generated insights. We provide examples and evidence from research studies to support our claims. Third, we examine the ways in which IoT contributes to the overall well-being of students by discussing the use of wearable devices and sensors to monitor physical health, safety measures and the creation of a conducive learning environment. We also explore how IoT can support mental health, foster healthy habits and provide remote access to educational resources. Fourth, we highlight the role of IoT in promoting the holistic development of students by discussing how IoT projects and initiatives empower students to develop essential skills such as problem-solving, critical thinking, creativity and digital literacy. We also explore the practical applications of IoT technology in preparing students for future careers and the digital age. Fifth, we offer insights and recommendations for educators, policymakers and researchers regarding the integration of IoT in education. We identify potential areas for further research, implementation strategies and policy development. We also discuss how IoT can be effectively leveraged to create healthier and more inclusive educational environments. Finally, we conclude by summarizing the key findings and contributions of the chapter, reiterating the transformative potential of IoT in education and well-being and emphasizing the need for continued exploration and research in this field.

6.2 Literature Review

IoT is a network of interconnected devices that can collect process and share data with each other and with humans. IoT has been applied in various domains, such as health, agriculture, transportation and manufacturing. In the field of education, IoT has the potential to transform teaching and learning processes by creating innovative and immersive learning environments that can be customized to individual needs and preferences. However, IoT also poses some challenges for

education, such as security, privacy, scalability and humanization. In this section, we will provide a comprehensive overview of the existing literature on IoT in education. The literature on IoT in education can be categorized into four main themes: (1) the use of IoT devices in early childhood education; (2) the use of IoT devices in higher education; (3) the impact of IoT technology on education in 2023; and (4) the role of IoT in education. We will summarize each theme below and provide a critical analysis of the existing studies.

6.3 The Use of IoT Devices in Early Childhood Education

Early childhood education (ECE) is the education of children from birth to eight years old. This stage is crucial for children's cognitive, social, emotional and physical development. IoT devices can enhance ECE by providing interactive and playful learning experiences for young children.

Several studies have explored the use of IoT devices in ECE settings and their effects on children's play, learning and growth. A common type of IoT device used in ECE settings is the IoT plaything, which is a physical object that can be connected to digital content or services via sensors or actuators. For example, Ling et al. (2022) conducted a systematic review of 22 articles on the use of IoT playthings in ECE settings. They found that IoT playthings were used for various purposes, such as enhancing children's literacy, numeracy, science, art and music skills; fostering children's creativity, imagination and expression; supporting children's social and emotional development; and facilitating children's exploration of digital and physical worlds. They also found that IoT playthings had positive influences on children's play, learning and growth, such as stimulating their interest and enthusiasm; providing them with feedback and guidance; enabling them to control their own learning pace and difficulty level; and encouraging them to be autonomous learners. However, they also identified some challenges and concerns related to the use of IoT playthings in ECE settings, such as high prices, data security issues, technical problems, pedagogical issues, ethical issues and parental involvement.

Another type of IoT device used in ECE settings is the educational robot, which is a programmable device that can move, sense and interact with the environment. Educational robots can be used to teach children various STEM-related skills, such as coding, logic, sequencing, patterns, geometry and physics. For example, Nikolopoulou (2022) conducted a literature review of 15 studies on the use of educational robots in ECE settings. She found that educational robots provided children with opportunities to engage in problem-solving, critical thinking and creativity. She also found that educational robots fostered children's collaboration, communication and social skills as they worked in groups to design and test their solutions. However, she also noted some challenges and limitations

related to the use of educational robots in ECE settings, such as technical difficulties, pedagogical issues, ethical issues and teacher training.

A third type of IoT device used in ECE settings is the simulation, which is a digital representation of a real-world phenomenon or system that can be manipulated and observed by the user. Simulations can be used to teach children various scientific concepts, such as gravity, magnetism, weather or ecology. For example, Dorouka et al. (2020) conducted a literature review of 12 studies on the use of simulations in ECE settings. They found that simulations enabled children to conduct experiments, test hypotheses and discover causal relationships. They also found that simulations enhanced children's motivation, engagement and learning outcomes. However, they also pointed out some challenges and drawbacks related to the use of simulations in ECE settings, such as technical issues, pedagogical issues, ethical issues and teacher support.

A fourth type of IoT device used in ECE settings is the digital game, which is an interactive application that provides feedback, challenges and rewards to the user. Digital games can be used to teach children various aspects of STEM, such as numbers, shapes, patterns, measurement and logic.

For example, Ling et al. (2022) conducted a systematic review of 18 studies on the use of digital games in ECE settings. They found that digital games improved children's cognitive, affective and psychomotor skills. They also found that digital games increased children's motivation, engagement and enjoyment. However, they also identified some challenges and risks related to the use of digital games in ECE settings, such as technical problems, pedagogical issues, ethical issues and parental involvement.

These are some of the types and purposes of IoT devices used in ECE settings and their influences on young children's play, learning and growth. The literature review shows that IoT devices can provide various benefits for ECE, such as enhancing learning experiences, facilitating data collection and analysis, improving classroom management and fostering collaboration and communication. However, the literature review also reveals some challenges and concerns related to the use of IoT devices in ECE settings, such as high prices, data security issues, technical problems, pedagogical issues, ethical issues and parental involvement. Therefore, the literature review suggests that there is a need for further research and practice to address these challenges and concerns and to optimize the use of IoT devices in ECE settings.

6.4 The Use of IoT Devices in Higher Education

Higher education is the education of students who have completed secondary education. Higher education can include undergraduate, postgraduate and doctoral studies. IoT devices can enhance higher education by providing flexible and adaptive learning environments that can support diverse learners and educators. Some examples of IoT devices used in higher education are as follows:

6.4.1 Smart Classrooms

These are classrooms that are equipped with IoT devices that can monitor and control various environmental factors, such as Lighting, Temperature, Humidity and Noise. Smart classrooms can also provide interactive features, such as smart boards, smart desks and smart projectors. Smart classrooms can improve the quality of teaching and learning by creating a comfortable and conducive learning environment for students and educators. For example, smart classrooms can adjust the lighting and temperature according to the preferences of the users or the time of the day. Smart classrooms can also enable remote access to educational resources and facilitate collaboration among students and educators (de La Guia et al., 2016).

6.4.2 Wearable Devices

These are devices that can be worn on the body or attached to clothing or accessories. Wearable devices can collect process and share data related to the user's physical activity, health status or location. Wearable devices can also provide feedback or guidance to the user through audio or visual signals. Wearable devices can enhance learning outcomes and well-being in higher education by providing personalized learning experiences, monitoring student performance and health and supporting student safety and security. For example, wearable devices can track student attendance, engagement and progress; provide real-time feedback and coaching; monitor student stress levels, heart rate and blood pressure; alert students or authorities in case of emergencies; and enable location-based services.

6.4.3 Smart Campus

This is a campus that is integrated with IoT devices that can collect process and share data related to various aspects of the campus environment, such as energy consumption, waste management, transportation, security and communication. Smart campus can also provide various services and facilities for students and smart dormitory. Smart campus can improve the efficiency and sustainability of campus operations by optimizing resource utilization, reducing energy consumption and waste generation and enhancing security and safety measures. Smart campus can also improve the quality of life and well-being of students and educators by providing convenient and accessible services and facilities, fostering social interaction and community engagement and creating a smart and connected learning environment (Dong et al., 2020).

These are some of the types and purposes of IoT devices used in higher education and their effects on teaching and learning processes. The literature review shows that IoT devices can provide various benefits for higher education, such as providing flexible and adaptive learning environments, supporting diverse learners and educators, facilitating data collection and analysis, improving campus

operations and sustainability and enhancing quality of life and well-being. Also, as reported by Dar et al. (2023), the transition from face-to-face to online teaching in teacher education during the COVID-19 pandemic has been a complex and challenging process that has required a rapid adaptation of pedagogical, technological and organizational aspects. However, the literature review also reveals some challenges and issues related to the use of IoT devices in higher education, such as security, privacy, scalability, reliability, interoperability, humanization and ethical issues. Also the conclusion of the paper by Dar and Nabi 2019 suggests that individuals who are not frequent internet users tend to possess emotional strength. Therefore, the literature review suggests that there is a need for further research and practice to address these challenges and issues and to optimize the use of IoT devices in higher education.

6.5 The Impact of IoT Technology on Education in 2023

IoT technology is constantly evolving and advancing, bringing new possibilities and opportunities for education. By 2023, IoT technology is expected to have a significant impact on education in various ways. Some of the predicted impacts of IoT technology on education in 2023 are as follows:

6.5.1 Increased Adoption of IoT Devices in Education

According to a report by Statista (2021), the global market size of IoT in education is expected to grow from 5.8 billion U.S. dollars in 2018 to 16.2 billion U.S. dollars in 2023. This indicates that more educational institutions will adopt IoT devices to enhance their teaching and learning processes. Moreover, more students and educators will use IoT devices for their personal or professional purposes, such as learning new skills, accessing educational resources or collaborating with peers or mentors.

6.5.2 Enhanced Personalization of Learning Experiences

IoT devices can enable personalized learning experiences by collecting and analyzing data related to students' learning preferences, needs, goals, progress and performance. Based on this data, IoT devices can provide customized content, feedback, guidance and support to students according to their individual needs and preferences. This can improve student engagement, motivation and learning outcomes. Moreover, IoT devices can enable adaptive learning environments that can adjust to the changing needs and preferences of students over time. For example, IoT devices can modify the difficulty level, pace, mode or sequence of learning activities based on students' performance and feedback. This can enhance student autonomy and self-regulation.

6.5.3 Improved Data-Driven Decision Making

IoT devices can collect and analyze large amounts of data related to various aspects of education, such as student performance, learning behavior, curriculum effectiveness, teacher quality, resource utilization and environmental factors. This data can provide valuable insights and information for educators, policymakers and researchers to make informed decisions and improve educational practices and policies. For example, IoT devices can provide real-time feedback and recommendations to educators on how to improve their teaching methods, curriculum design or classroom management. IoT devices can also provide evidence-based reports and evaluations to policymakers and researchers on the impact and effectiveness of educational interventions, programs or policies.

6.5.4 Increased Collaboration and Communication

IoT devices can facilitate collaboration and communication among students, educators and other stakeholders in education. IoT devices can enable seamless connectivity and interaction among different devices, platforms and networks. This can allow students and educators to access, share and exchange educational resources, data and information anytime and anywhere. Moreover, IoT devices can support synchronous and asynchronous communication modes, such as voice calls, video conferencing, instant messaging or social media. This can enable students and an educator to communicate and collaborate with peers or mentors across different locations, time zones or cultures.

6.5.5 Enhanced Innovation and Creativity

IoT devices can foster innovation and creativity in education by providing students and educators with opportunities to explore experiment and create with digital and physical materials. IoT devices can also stimulate students' curiosity and imagination by exposing them to new experiences, perspectives and possibilities. Furthermore, IoT devices can empower students and educators to design and develop their own IoT solutions to address real-world problems or challenges. This can enhance their problem-solving, critical thinking and creativity skills.

These are some of the predicted impacts of IoT technology on education in 2023. The literature review shows that IoT technology can have a significant impact on education in various ways, such as increasing the adoption of IoT devices in education, enhancing the personalization of learning experiences, improving data-driven decision making, increasing collaboration and communication and enhancing innovation and creativity. However, the literature review also indicates some challenges and issues related to the impact of IoT technology on education in 2023 such as security, privacy, scalability, reliability, interoperability, humanization and ethical issues. Therefore, the literature review suggests that there

is a need for further research and practice to address these challenges and issues and to optimize the impact of IoT technology on education in 2023.

6.6 The Role of IoT in Education

IoT has a significant role in education, as it can enhance teaching and learning processes, improve educational outcomes and well-being and promote holistic development. However, IoT also has some limitations and risks that need to be considered and addressed. In this section, we will discuss the role of IoT in education from different perspectives: students, educators, policymakers and researchers.

6.6.1 Students

IoT can benefit students by providing them with personalized learning experiences that can cater to their individual needs and preferences. IoT can also improve students' academic performance by providing them with real-time feedback and guidance. Moreover, IoT can enhance students' well-being by monitoring their physical health and safety, supporting their mental health and fostering healthy habits. Furthermore, IoT can promote students' holistic development by empowering them to develop essential skills such as problem-solving, critical thinking, creativity and digital literacy. However, IoT also poses some risks for students, such as privacy invasion, data misuse, cyber bullying, addiction or distraction. According to Syed and Dar (2022), IOT alone cannot guarantee productive and holistic learning; students still need a human element in technology enhanced environment. Therefore, students need to be aware of the benefits and risks of using IoT devices and learn how to use them responsibly and ethically.

6.6.2 Educators

IoT can benefit educators by providing them with flexible and adaptive learning environments that can support diverse learners and educators. IoT can also improve educators' teaching quality by providing them with real-time data and insights that can inform their instructional strategies. Moreover, IoT can enhance educators' well-being by reducing their workload and stress, improving their communication and collaboration and enabling their professional development. Furthermore, IoT can promote educators' innovation and creativity by providing them with opportunities to explore experiment and create with digital and physical materials. However, IoT also poses some challenges for educators, such as technical difficulties, pedagogical issues, ethical issues and teacher training. Therefore, educators need to be prepared and supported to integrate IoT devices into their teaching and learning processes and to address the challenges and issues that may arise.

6.6.3 Policymakers

IoT can benefit policymakers by providing them with evidence-based reports and evaluations that can inform their policy development and implementation. IoT can also improve policymakers' policy effectiveness by providing them with real-time feedback and recommendations that can help them monitor and evaluate their policy outcomes and impacts. Moreover, IoT can enhance policymakers' policy sustainability by providing them with data and information that can help them optimize resource utilization, reduce energy consumption and waste generation and enhance security and safety measures. Furthermore, IoT can promote policymakers' policy innovation and creativity by providing them with data and information that can help them identify new opportunities and possibilities for education. However, IoT also poses some issues for policymakers, such as security, privacy, scalability, reliability, interoperability and ethical issues. Therefore, policymakers need to collaborate with educators, researchers and technology developers to ensure the responsible and ethical use of IoT devices in education and to address the issues that may arise.

6.6.4 Researchers

IoT can benefit researchers by providing them with large amounts of data and information that can inform their research questions and hypotheses. IoT can also improve researchers' research quality by providing them with real-time data and information that can help them conduct experiments, test hypotheses and discover causal relationships. Moreover, IoT can enhance researchers' research impact by providing them with data and information that can help them disseminate their research findings and recommendations to various stakeholders in education. Furthermore, IoT can promote researchers' research innovation and creativity by providing them with data and information that can help them identify new research gaps and areas for further research. However, IoT also poses some challenges for researchers, such as security, privacy, scalability, reliability, interoperability and ethical issues. Technology applications as recommended by Syed and Dar (2022) should be grounded in purposeful research. Therefore, researchers need to collaborate with educators, policymakers and technology developers to ensure the responsible and ethical use of IoT devices in education and to address the challenges and issues that may arise.

These are some of the perspectives on the role of IoT in education. The literature review shows that IoT has a significant role in education, as it can enhance teaching and learning processes, improve educational outcomes and well-being and promote holistic development. However, the literature review also indicates some limitations and risks of IoT in education, such as security, privacy, scalability, reliability, interoperability, humanization and ethical issues. Therefore, the literature review suggests that there is a need for further research and practice to address these limitations and risks and to optimize the role of IoT in education.

6.7 Impact on Academic Outcomes

One of the main influences of IoT on education is its impact on academic outcomes. Academic outcomes refer to the measurable results of students' learning, such as grades, test scores, retention rates, graduation rates and employability. IoT devices, applications and platforms can enhance academic outcomes in education by providing personalized learning experiences, real-time data analysis and instructional strategies informed by IoT-generated insights. In this section, we will discuss how IoT can enhance academic outcomes in education by providing examples and evidence from research studies.

6.8 Personalized Learning Experiences

Personalized learning experiences are learning experiences that are tailored to the individual needs, preferences, goals and abilities of each student. Personalized learning experiences can improve student engagement, motivation and learning outcomes by providing customized content, feedback, guidance and support. IoT devices can enable personalized learning experiences by collecting and analyzing data related to students' learning patterns, preferences and behaviors. Based on this data, IoT devices can provide customized content, feedback, guidance and support to students according to their individual needs and preferences. This level of customization can improve student engagement, motivation and learning outcomes. For example, a study by Khanafer et al. (2019) explored the effects of an IoT-based personalized learning environment on students' academic performance and satisfaction in a high school mathematics course. The environment consisted of smart devices, such as tablets, smart boards and smart watches, that collected data from students' learning activities, such as attendance, participation, quiz scores and feedback ratings. Based on this data, the environment provided personalized learning content and feedback to each student according to their learning level and style. The results showed that the students who used the IoT-based personalized learning environment had significantly higher academic performance and satisfaction than the students who used a traditional learning environment.

These are some examples of how IoT devices can enable personalized learning experiences by collecting and analyzing data related to students' learning patterns, preferences and behaviors. The literature review shows that personalized learning experiences can improve student engagement, motivation and learning outcomes by providing customized content, feedback, guidance and support. However, the literature review also indicates some challenges and issues related to personalize learning experiences using IoT devices, such as security, privacy, ethical and pedagogical issues. Therefore, the literature review suggests that there is a need for further research and practice to address these challenges and issues and to optimize personalized learning experiences using IoT devices.

6.9 Real-Time Data Analysis

Real-time data analysis is the process of collecting, processing and analyzing data as soon as it is generated or received. Real-time data analysis can provide timely and accurate insights and information for decision making and action taking. IoT devices can enable real-time data analysis by collecting and transmitting large amounts of data from various sources, such as sensors, actuators, cameras or wearables. IoT devices can also process and analyze the data using advanced techniques, such as machine learning, artificial intelligence or deep learning. This can provide useful insights and information for improving teaching and learning processes, such as student performance, learning behavior, curriculum effectiveness, teacher quality or resource utilization.

For example, a study by Yan et al. (2019) investigated the use of IoT devices for real-time data analysis in education. They used smart wristbands and eye-tracking technology to collect data from students' learning activities, such as attendance, participation, quiz scores and feedback ratings. They also used sensors to collect data from the environmental factors, such as Lighting, Temperature, Humidity and Noise. Based on this data, they performed real-time data analysis using machine learning and deep learning techniques to provide insights and information on how students' attention affects their results. They found that there was a correlation between eye tracking, heart rate and student attention and how it all impacts their learning outcomes.

Another example is a study by Okada et al. (2023) that explored the use of IoT devices for real-time data analysis in education. They used wearable devices and sensors to collect data from students' real-world experiences, such as location, movement, activity and emotion. They also used smartphones to collect data from students' digital activities, such as browsing history, app usage and social media interactions. Based on this data, they performed real-time data analysis using artificial intelligence and deep learning techniques to provide insights and information on how students' self-regulation process of real-world experiences affects their learning outcomes.

These are some examples of how IoT devices can enable real-time data analysis by collecting and transmitting large amounts of data from various sources and processing and analyzing the data using advanced techniques. The literature review shows that real-time data analysis can provide timely and accurate insights and information for improving teaching and learning processes. However, the literature review also indicates some challenges and issues related to real-time data analysis using IoT devices, such as security, instructional Strategies Informed by IoT-Generated Insights.

Instructional strategies are the methods and techniques used by educators to facilitate teaching and learning processes. Instructional strategies can improve student engagement, motivation and learning outcomes by providing appropriate content, activities and feedback. IoT devices can enable instructional strategies

informed by IoT-generated insights by providing real-time data and information that can help educators design and deliver effective and efficient instruction. IoT devices can also provide real-time feedback and recommendations to educators on how to improve their instructional methods, curriculum design or classroom management.

For example, a study by De La Guia et al. (2016) investigated the use of IoT devices for instructional strategies informed by IoT-generated insights in education. They used smart classrooms to collect data from students' learning activities, such as attendance, participation, quiz scores and feedback ratings. They also used sensors to collect data from the environmental factors, such as Lighting, Temperature, Humidity and Noise. Based on this data, they performed real-time data analysis using machine learning techniques to provide insights and information on how to optimize the learning environment for students. They also provided real-time feedback and recommendations to educators on how to adjust the environmental factors, such as lighting and temperature, according to the preferences of the students.

Another example is a study by Khanafer et al. (2019) that explored the use of IoT devices for instructional strategies informed by IoT-generated insights in education. They used educational robots to collect data from students' learning activities, such as coding, logic, sequencing and patterns. They also used sensors to collect data from the environmental factors, such as light intensity and sound level. Based on this data, they performed real-time data analysis using artificial intelligence techniques to provide insights and information on how to enhance students' learning outcomes. They also provided real-time feedback and recommendations to educators on how to modify the difficulty level, pace, mode or sequence of learning activities based on students' performance and feedback.

These are some examples of how IoT devices can enable instructional strategies informed by IoT-generated insights by providing real-time data and information that can help educators design and deliver effective and efficient instruction. The literature review shows that instructional strategies informed by IoT-generated insights can improve student engagement, motivation and learning outcomes by providing appropriate content, activities and feedback.

6.10 Conclusion

The Internet of Things (IoT) is a phenomenon that connects physical objects with sensors and actuators to computing systems via wired or wireless networks. IoT has a significant impact on education, as it can enhance teaching and learning processes, improve educational outcomes and well-being and promote holistic development. However, IoT also has some limitations and risks that need to be considered and addressed. In this literature review, we have discussed the impact of IoT on education from different perspectives: students, educators, policymakers and researchers. We have also discussed the role of IoT in education from different aspects: types and purposes of IoT devices, personalized learning experiences, real-time data analysis

and instructional strategies informed by IoT-generated insights, educational outcomes and well-being and holistic development.

We have found that IoT devices can provide various benefits for education, such as providing flexible and adaptive learning environments, supporting diverse learners and educators, facilitating data collection and analysis, improving campus operations and sustainability and enhancing quality of life and well-being. We have also found that IoT devices can foster innovation and creativity in education by providing students and educators with opportunities to explore experiment and create with digital and physical materials. Moreover, we have found that IoT devices can empower students and educators to design and develop their own IoT solutions to address real-world problems or challenges.

However, we have also found that there are some challenges and issues related to the use of IoT devices in education, such as security, privacy, scalability, reliability, interoperability, humanization and ethical issues. These challenges and issues may hinder the adoption and implementation of IoT devices in education or cause negative consequences for students, educators or other stakeholders. Therefore, we have suggested that there is a need for further research and practice to address these challenges and issues and to optimize the use of IoT devices in education.

In conclusion, we have shown that IoT is a powerful technology that can transform education in various ways. However, we have also shown that IoT is not a panacea that can solve all the problems or challenges in education. Rather, IoT is a tool that needs to be used wisely and responsibly by students, educators, policymakers and researchers. By doing so, we believe that IoT can create a smarter and better future for education.

References

- Dar, M. A., & Nabi, S. (2019). Emotional Intelligence of Regular and Non-Regular Internet Users—A Study on University Students. *Insight Journal of Applied Research in Education*, 24(1), 271–278.
- Dar, M.A., Parveen, A., Rasool, I., & Jan, S. (2023). Transition from Face-To-Face to Online Teaching in Teacher Education during Covid-19 Pandemic: A Systematic Review. *Insight Journal of Applied Research in Education*, 28(1), 21–43.
- de la Guia, E., Camacho, V. L., Orozco-Barbosa, L., Lujan, V. M. B., Penichet, V. M., & Pérez, M. L. (2016). Introducing IoT and Wearable Technologies into Task-Based Language Learning for Young Children. *IEEE Transactions on Learning Technologies*, 9(4), 366–378. 10.1109/TLT.2016.2557333
- Dong, Z. Y., Zhang, Y., Yip, C., Swift, S., & Beswick, K. (2020). Smart Campus: Definition, Framework, Technologies, and Services. *IET Smart Cities*, 2(1), 43–54. 10.1049/iet-smc.2019.0072
- Dorouka, P., Papadakis, S., & Kalogiannakis, M. (2020). Tablets and Apps for Promoting Robotics, Mathematics, STEM Education and Literacy in Early Childhood Education. *International Journal of Mobile Learning and Organisation*, 14(2), 255–274. 10.1504/IJMLO.2020.106179

- Khanafer, M., & El-Abd, M. (2019, April). Guidelines for Teaching an Introductory Course on the Internet of Things. In *2019 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1488–1492). IEEE. 10.1109/EDUCON.2019.8725186
- Ling, L., Yelland, N., Hatzigianni, M., & Dickson-Deane, C. (2022). The Use of Internet of Things Devices in Early Childhood Education: A Systematic Review. *Education and Information Technologies*, 27(5), 6333–6352. 10.1007/s10639-021-10872-x
- Nikolopoulou, K. (2022). Digital Technology in Early STEM Education: Exploring Its Supportive Role. In *STEM, Robotics, Mobile Apps in Early Childhood and Primary Education: Technology to Promote Teaching and Learning* (pp. 103–115). Singapore: Springer Nature Singapore. 10.1007/978-981-19-0568-1_6
- Okada, M., Nagata, K., Watanabe, N., & Tada, M. (2023). Computational Learning Analytics to Estimate Location-based Self-regulation Process of Real-world Experiences. *IEEE Transactions on Learning Technologies*. 10.1109/TLT.2023.3262598
- Statista. (2021). www.statista.com
- Syed, N. A., & Dar, M. A. (2022). Innovations in Education Is in Misapprehension: A Theoretical Review. *National Journal of Education*, XX(1), 19–29. <http://www.njebhu.in/jan%202022%20issue.pdf>
- Yan, S., Lin, K. J., Zheng, X., & Zhang, W. (2019). Using Latent Knowledge to Improve Real-Time Activity Recognition for Smart IoT. *IEEE Transactions on Knowledge and Data Engineering*, 32(3), 574–587. 10.1109/TKDE.2019.2891659

Chapter 7

Integration of Unmanned Aerial Vehicles (UAVs) and IoT for Crop Monitoring and Spraying

Tarun Kumar Vashishth, Vikas Sharma,
Kewal Krishan Sharma, Sachin Chaudhary,
Bhupendra Kumar, and Rajneesh Panwar

School of Computer Science and Application, IIMT University, Meerut, Uttar Pradesh, India

7.1 Introduction

The integration of Unmanned Aerial Vehicles (UAVs) and the Internet of Things (IoT) has revolutionized the agricultural industry, offering new possibilities for precision farming and enhancing crop monitoring and spraying practices. UAVs, commonly known as drones, equipped with advanced sensors and cameras, provide a bird's-eye view of agricultural fields, enabling farmers and agronomists to monitor crops with unprecedented detail. The IoT, on the other hand, connects these UAVs with a network of sensors and devices, facilitating gathering, analysis, and making choices of data in actual time. The importance, benefits, and potential drawbacks of integrating UAVs and IoT for crop monitoring and spraying are highlighted in this chapter.

7.1.1 Overview of the Integration of UAVs and IoT in Agriculture

The integration of Unmanned Aerial Vehicles (UAVs) and the Internet of Things (IoT) has brought about transformative changes in the agricultural industry. This integration combines the capabilities of UAVs, also known as drones, with IoT technologies, enabling precision farming, improved crop monitoring, and efficient spraying practices. By leveraging UAVs and IoT, farmers and agronomists can gather real-time data, make data-driven decisions, and optimize agricultural operations in a more effective and sustainable manner (Figure 7.1).

UAVs have emerged as powerful tools in agriculture, offering the ability to capture aerial imagery and collect data with high resolution and accuracy. Equipped with cameras, sensors, and GPS systems, UAVs can fly over agricultural fields and collect data on various parameters such as crop health, growth patterns, soil moisture levels, temperature, humidity, and vegetation indices. With the use of this thorough information, farmers may better understand the general health of their crops and identify illnesses, nutrient deficits, and pest infestations early on. UAVs can efficiently and swiftly cover wide tracts of agriculture, saving time and manpower normally needed for conventional inspections.

The IoT, on the other hand, connects devices and sensors through a network, allowing for seamless data communication and analysis. In the context of agriculture, IoT devices include soil moisture sensors, weather stations, pest detection sensors, and crop health monitoring systems. By integrating UAVs with IoT devices, real-time data collection becomes possible, enabling farmers to monitor and analyze key parameters affecting crop health. The collected data can be transmitted to a central hub or cloud-based platform for analysis and visualization, providing farmers with actionable insights and decision support.

The integration of UAVs with IoT further enhances the potential of these aerial platforms. By integrating IoT sensors with UAVs, farmers and agronomists gain access to a wealth of real-time data, enabling them to make timely and data-driven decisions. For instance, soil moisture sensors can provide information on the

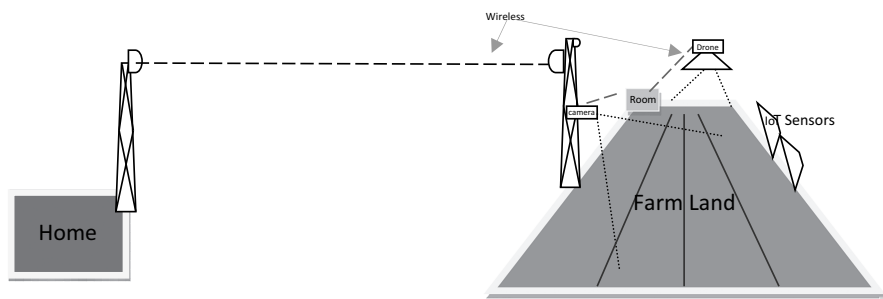


Figure 7.1 IoT and UAV connectivity to monitor crops, remotely.

irrigation needs of crops, weather sensors can relay up-to-date weather conditions, and pest detection sensors can identify the presence of harmful insects or diseases. This integration allows for precision agriculture, where resources such as water, fertilizers, and pesticides can be applied in a targeted manner, reducing waste and minimizing environmental impact.

In conclusion, the integration of UAVs and IoT in agriculture offers immense potential for improving crop monitoring, management, and spraying practices. By combining the capabilities of UAVs for aerial data collection and IoT for real-time data analysis, farmers can make informed decisions, optimize resource allocation, and enhance overall productivity in a more sustainable manner. Continued advancements in UAV and IoT technologies, along with regulatory frameworks and industry collaborations, will further drive the adoption and effectiveness of this integration in the agricultural sector.

7.1.2 Importance of Crop Monitoring and Spraying in Modern Agriculture

Crop monitoring and spraying play a crucial role in modern agriculture, contributing to improved crop health, increased productivity, and sustainable farming practices. Here are the key reasons highlighting the importance of crop monitoring and spraying in modern agriculture.

7.1.2.1 Early Detection of Crop Issues

Crop monitoring allows farmers to identify and diagnose crop diseases, nutrient deficiencies, weed infestations, and pest outbreaks at an early stage. Early detection enables timely interventions and prevents the spread of problems, minimizing crop losses and optimizing yield potential.

7.1.2.2 Precision Farming and Resource Optimization

Crop monitoring provides valuable insights into the spatial variability of crop conditions within a field. This information allows farmers to implement precision farming techniques, such as variable rate application of fertilizers, pesticides, and water. By tailoring inputs to specific crop needs, farmers can optimize resource allocation, reduce waste, and enhance efficiency.

7.1.2.3 Improved Pest and Disease Management

Timely and accurate monitoring of pests and diseases is crucial for effective control measures. By monitoring crop health and pest populations, farmers can implement targeted spraying strategies, minimizing the use of pesticides and reducing the risk

of resistance development. This approach promotes environmentally friendly farming practices and reduces the impact on beneficial organisms.

7.1.2.4 Optimized Crop Nutrition

Crop monitoring helps in assessing nutrient levels and imbalances in the soil. Farmers can apply fertilizer effectively through tracking elements including soil moisture, pH, and nutrient level, ensuring that crops receive the required nutrients for healthy growth. This optimization leads to improved crop quality and yield.

7.1.2.5 Environmental Sustainability

Crop monitoring and precise spraying practices contribute to environmental sustainability in agriculture. By accurately assessing crop needs and targeting inputs, farmers can reduce the overall use of pesticides, fertilizers, and water, minimizing their impact on ecosystems and groundwater resources. This approach promotes sustainable farming practices and mitigates potential environmental risks.

7.1.3 Limitations and Usefulness of Using UAVs and IoT for Crop Management

Using Unmanned Aerial Vehicles (UAVs) and the Internet of Things (IoT) for crop management offers several potential benefits, but it also presents certain challenges. Here, we explore the potential benefits and challenges associated with the utilization of UAVs and IoT in crop management:

Benefits:

- i. **Enhanced Crop Monitoring:** Using high-resolution device can capture aerial imagery, collect data on crop health, growth patterns, and environmental conditions, providing farmers with valuable insights for timely decision-making and proactive crop management
- ii. **Precision Farming:** The integration of UAVs and IoT facilitates precision farming practices. By collecting data on various parameters, farmers can precisely tailor their irrigation, fertilization, and other management practices to meet the specific needs of different areas within a field. This leads to optimized resource allocation, reduced waste, and increased efficiency.
- iii. **Early Detection of Crop Issues:** UAVs combined with IoT sensors allow for early detection of crop diseases, nutrient deficiencies, and pest infestations. The ability to identify such issues at their initial stages enables farmers to implement timely and targeted interventions, minimizing crop losses and increasing overall yield potential.

- iv. **Improved Spraying Efficiency:** UAVs can be equipped with spraying systems that enable targeted and precise pesticide application. By integrating IoT sensors, farmers can identify specific areas affected by pests or diseases, ensuring that spraying is focused only where necessary. This reduces the overall use of pesticides, minimizes environmental impact, and increases the effectiveness of pest management.
- v. **Collection and Analysis of Current Information:** The fusion of IoT and Drones enables real-time data collection, transmission, and analysis. This allows farmers to access up-to-date information on crop conditions, weather patterns, and other relevant factors. Real-time data facilitates prompt decision-making, helping farmers respond quickly to changing conditions and optimize their management strategies.

Challenges:

- i. **Regulatory and Legal Considerations:** The use of UAVs in agriculture is subject to airspace regulations and legal restrictions. Compliance with regulations related to flight operations, privacy concerns, and data ownership needs to be ensured to enable the safe and responsible use of UAVs and IoT in crop management.
- ii. **Data Security and Privacy:** Collecting and transmitting data from UAVs and IoT sensors raise concerns regarding data security and privacy. Measures must be in place to protect the integrity and confidentiality of the collected data, ensuring that it is not vulnerable to unauthorized access or misuse.
- iii. **Interoperability and Standardization:** The integration of UAVs and IoT devices from various manufacturers may present challenges related to interoperability and standardization. Establishing common communication protocols, data formats, and compatibility standards is essential to facilitate seamless integration and data exchange between different systems.
- iv. **Skill and Knowledge Requirements:** Utilizing UAVs and IoT technologies in crop management requires a certain level of technical knowledge and expertise. Farmers and agronomists need to be trained on the operation of UAVs, data collection methods, and data analysis techniques to effectively leverage these technologies for optimal results.
- v. **Initial Investment and Maintenance:** Adopting UAVs and implementing IoT systems for crop management involves initial investment costs. Procuring UAVs, sensors, and other equipment, as well as ensuring regular maintenance, can impose financial burdens on farmers. However, the long-term benefits and potential return on investment should be considered in evaluating the feasibility of adopting these technologies.
- vi. **Environmental Considerations:** While UAVs and IoT can contribute to more sustainable farming practices, their environmental impact should be

carefully assessed. Factors such as energy consumption, noise pollution, and the potential risks associated with chemical spraying need to be taken into account to minimize negative environmental consequences.

7.2 Literature Review

The integration of Unmanned Aerial Vehicles (UAVs) and the Internet of Things (IoT) has shown promising applications in various fields, including agriculture. This literature review aims to provide an overview of the research conducted on the integration of UAVs and IoT for crop monitoring and spraying. By combining UAVs' capabilities for aerial surveillance and data collection with IoT's connectivity and sensor technologies, farmers can improve their crop management practices, enhance yield, and optimize resource utilization.

Saha et al. [1] proposed solutions related to these drones, if integrated with various Machine Learning and Internet of Things concepts, can help in increasing the scope of further improvement. In this paper, the related work in this field has been highlighted along with proposed solutions that can be integrated into the drone using Raspberry Pi 3 B module.

Boursianis et al. [2] provide an extensive overview of the integration of IoT and UAV technologies for smart farming applications. The authors explore the potential of combining IoT and UAVs to enhance agricultural practices, improve crop productivity, and enable precision farming. The paper explores the challenges and opportunities associated with the adoption of IoT and UAV technologies in agriculture. It addresses issues related to data security, privacy, energy efficiency, and regulatory frameworks, while also discussing the potential benefits in terms of resource optimization, cost reduction, and increased yields. Additionally, the authors provide insights into the future trends and advancements in the field, including the use of artificial intelligence, machine learning, and edge computing in IoT-UAV systems for intelligent decision-making in farming operations. Overall, this comprehensive review serves as a valuable resource for researchers, practitioners, and policymakers interested in understanding the integration of IoT and UAV technologies in smart farming and the potential benefits they offer for sustainable and efficient agricultural practices.

Singh and Sharma [3] present experimental results and case studies to demonstrate the effectiveness of the proposed framework in improving precision agriculture practices. They discuss the advantages of using WSN and UAV technologies, including real-time monitoring, cost-effectiveness, and scalability. The paper highlights the potential of the intelligent WSN-UAV-based IoT framework for precision agriculture applications. The integration of WSN, UAVs, and IoT enables farmers to make informed decisions based on real-time data, leading to optimized resource utilization, enhanced crop quality, and increased agricultural productivity.

Maddikunta et al. [4] provide an in-depth exploration of the applications, requirements, and challenges associated with the use of unmanned aerial vehicles

(UAVs) in smart agriculture. The authors discuss the various applications of UAVs in agriculture, including crop monitoring, precision agriculture, yield estimation, pest and disease detection, irrigation management, and livestock monitoring. They highlight the advantages of UAVs, such as their ability to provide real-time and high-resolution data, cover large areas efficiently, and access hard-to-reach locations. In conclusion, the paper highlights the immense potential of UAVs in transforming agriculture into a smart and data-driven industry. The authors underline the importance of addressing the challenges and requirements to facilitate the widespread adoption and successful integration of UAVs in smart agriculture applications.

Bhuvaneshwari et al. [5] discuss the challenges and limitations associated with the implementation of the IoT-based UAV system. These challenges include connectivity issues, power management, data security, and the need for trained personnel. The paper emphasizes the importance of addressing these challenges to ensure the successful adoption of the technology.

Velusamy et al. [6] highlight the potential solutions and advancements in UAV technology that can help overcome these challenges. They discuss the integration of UAVs with other technologies, such as Internet of Things (IoT), Artificial Intelligence (AI), and machine learning, to enhance data analysis and decision-making processes in precision agriculture. The paper emphasizes the promising role of UAVs in precision agriculture and their potential to revolutionize farming practices. The authors encourage further research and development in UAV technology to address the challenges and maximize the benefits of UAVs in achieving sustainable and efficient agriculture.

Wang et al. [7] present an overview of the progress and applications of agricultural UAVs in China and discuss the prospects and challenges for their use in Polish agriculture. The authors highlight the potential benefits of UAVs in improving farming practices and encourage further research and collaboration to harness the full potential of UAV technology in agriculture.

The integration of Unmanned Aerial Vehicles (UAVs) and the Internet of Things (IoT) offers significant potential for crop monitoring and spraying in agriculture. The reviewed studies demonstrate the benefits of using UAVs for aerial data collection, combined with IoT sensors and connectivity, to enable real-time monitoring of crop health, disease identification, pest detection, and optimized resource management. Further research and development in this area are expected to advance the implementation of UAV-IoT systems for improved crop management and increased agricultural productivity.

7.3 Unmanned Aerial Vehicles (UAVs) in Agriculture

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have emerged as powerful tools in the field of agriculture. These aerial platforms equipped with advanced sensors, cameras, and GPS capabilities offer a range of applications and

benefits for farmers and agronomists. Here, we explore the use of UAVs in agriculture and their potential impact on various aspects of farming:

7.3.1 Crop Monitoring and Assessment

UAVs provide a bird's-eye view of agricultural fields, enabling farmers to monitor crops with high-resolution imagery and collect valuable data. They can capture aerial images, multispectral or hyperspectral data, and thermal images, allowing for detailed analysis of crop health, growth patterns, and stress conditions. This information helps in assessing crop performance, detecting diseases, nutrient deficiencies, and pest infestations, and making informed decisions about interventions.

7.3.2 Precision Agriculture

UAVs facilitate precision agriculture practices by gathering data on the variability of crop conditions within a field. By integrating GPS technology and onboard sensors, they can precisely map variations in soil moisture, nutrient levels, and plant health. This data enables farmers to implement site-specific management strategies, such as variable rate application of fertilizers, pesticides, and water, optimizing resource utilization, and reducing input costs.

7.3.3 Crop Mapping and Inventory

UAVs can generate detailed crop maps and 3D models of agricultural fields, providing valuable information on plant density, canopy cover, and spatial distribution. These maps assist in assessing crop biomass, estimating yield potential, and identifying areas requiring targeted interventions. Crop inventories conducted using UAVs help in monitoring changes in crop growth over time and facilitate better crop management decisions.

7.3.4 Irrigation Management

UAVs equipped with thermal sensors can identify variations in crop water stress, helping farmers optimize irrigation strategies. By detecting areas with inadequate or excessive moisture levels, UAVs enable targeted irrigation applications, preventing water waste and ensuring proper water distribution across the field (Figure 7.2).

7.3.5 Crop Spraying and Pest Management

UAVs equipped with spraying systems offer an efficient and targeted approach to crop protection. With precise navigation and the ability to spray specific areas, they minimize pesticide usage and reduce environmental impact. UAVs can also aid in

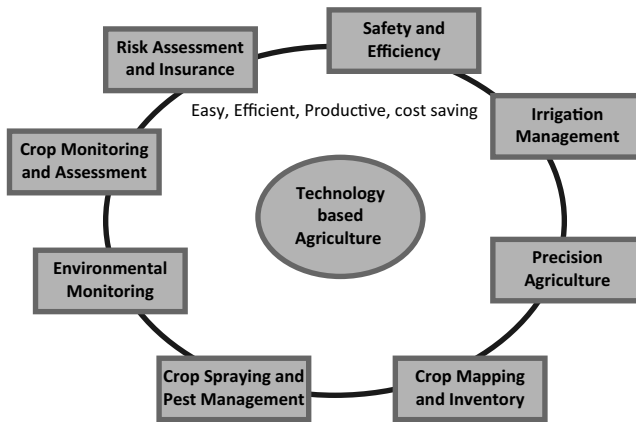


Figure 7.2 Technology based agriculture, same recurring cost, crop failure, time, and unnecessary hard work.

pest monitoring and early detection, allowing for timely interventions and effective pest management strategies.

7.3.6 Environmental Monitoring

UAVs can contribute to environmental monitoring in agricultural settings. They can be used to assess soil erosion, monitor water bodies, and detect pollution sources. This information assists in identifying areas of concern, implementing appropriate mitigation measures, and promoting sustainable land and water management practices.

7.3.7 Risk Assessment and Insurance

UAVs provide valuable data for risk assessment and insurance purposes in agriculture. They can assess crop damage caused by natural disasters, diseases, or pests, allowing for accurate claim evaluations and insurance coverage determination.

7.3.8 Safety and Efficiency

UAVs offer the advantage of being able to access difficult-to-reach or hazardous areas, reducing risks to human operators. They can cover large areas quickly, collecting data more efficiently than traditional ground-based methods. This efficiency leads to time and labor savings, enabling farmers to monitor larger areas in a shorter period.

In conclusion, by giving farmers useful insights, improved data-gathering capabilities, and precise management tools, Drones have transformed agriculture.

From crop monitoring and assessment to precision agriculture practices and environmental monitoring, UAVs offer numerous benefits that can contribute to improved crop productivity, resource efficiency, and sustainability in the agricultural industry.

7.4 Internet of Things (IoT) in Agriculture

The Internet of Things (IoT) is playing an increasingly significant role in agriculture, revolutionizing traditional farming practices and enabling the development of smart, connected agricultural systems. By integrating sensors, devices, and connectivity, IoT technology offers numerous applications and benefits for the agricultural sector. Here, we explore the use of IoT in agriculture and its potential impact on various aspects of farming.

7.4.1 Precision Agriculture

IoT enables precision agriculture practices by collecting real-time data on soil moisture, temperature, humidity, and other environmental parameters. These data points, gathered through sensors placed in fields, provide farmers with valuable insights into the spatial variability of conditions.

7.4.2 Smart Irrigation

IoT-based irrigation systems help farmers achieve efficient water management. Soil moisture sensors placed at different depths provide accurate information about the water content in the soil. This data is transmitted wirelessly to the farmers, who can then automate or remotely control irrigation systems, ensuring that the ideal amount of water is applied to crops at the appropriate moment. Smart irrigation reduces water consumption, minimizes runoff, and improves crop health.

7.4.3 Livestock Monitoring

IoT devices can monitor the health and well-being of livestock. Wearable sensors can track parameters such as body temperature, heart rate, and movement patterns. This information helps farmers identify signs of illness or distress in animals, enabling timely intervention. IoT-based livestock monitoring systems enhance animal welfare, improve breeding programs, and increase overall productivity.

7.4.4 Crop Health Monitoring

IoT sensors can monitor crop health parameters such as temperature, humidity, light levels, and air quality. Continuous monitoring allows farmers to detect early

signs of stress, diseases, or pests, facilitating proactive management practices. By leveraging IoT data, farmers can optimize the timing and dosage of pesticide applications, reducing chemical usage and minimizing environmental impact.

7.4.5 Weather Monitoring and Forecasting

IoT-based weather stations provide accurate and localized weather data specific to farm locations. This information assists farmers in making informed decisions regarding planting, harvesting, and crop protection activities. Real-time weather monitoring combined with historical data allows for better crop planning and risk management.

7.5 Crop Monitoring with UAVs and IoT

Crop monitoring includes combination of UAVs and IoT which offers a powerful solution for farmers to gather real-time, high-resolution data on crop health, growth, and environmental conditions. This combination provides several benefits and advancements in crop monitoring practices. Here, we delve into the details of crop monitoring with UAVs and IoT.

7.5.1 Aerial Imaging and Sensing

UAVs equipped with cameras, multispectral or hyperspectral sensors, and thermal cameras capture high-resolution aerial images and collect data on crop health parameters. These sensors can detect variations in vegetation vigor, chlorophyll content, water stress, and pest infestations. The collected data is transmitted to the IoT platform for analysis and interpretation.

7.5.2 Real-Time Monitoring

UAVs equipped with IoT connectivity enable real-time data transmission, allowing farmers to monitor crops continuously. The collected data, such as images and sensor readings, is instantly accessible on a connected device. Real-time monitoring provides immediate insights into crop conditions, enabling proactive decision-making and timely interventions.

7.5.3 Spatial and Temporal Crop Variability

The combination of UAVs and IoT helps farmers understand the spatial variability of crop conditions within a field. By collecting data at multiple locations, farmers can identify variations in plant health, nutrient levels, and water stress. Over time, the continuous monitoring enables the analysis of temporal changes and the identification of trends and patterns in crop growth and development.

7.5.4 Early Detection of Crop Issues

UAVs equipped with sensors and cameras enable early detection of crop diseases, nutrient deficiencies, and pest infestations. By regularly monitoring crops, farmers can identify subtle changes in plant health and take proactive measures to mitigate the impact of potential threats. Early detection allows for timely interventions, reducing crop losses and optimizing yield potential.

7.5.5 Integration with Other Agricultural Technologies

The integration of UAVs and IoT with other agricultural technologies, such as GPS-guided machinery and automated irrigation systems, enables seamless data exchange and decision-making processes. This integration promotes the concept of a connected farm ecosystem, where data from different sources is combined to enhance overall farm management.

7.6 Crop Spraying with UAVs and IoT

By combining UAVs equipped with spraying systems and IoT connectivity, farmers can achieve targeted and efficient crop spraying, resulting in reduced chemical usage, minimized environmental impact, and improved crop health. Here, we explore the details of crop spraying with UAVs and IoT (Figure 7.3).

7.6.1 Precision Application

UAVs equipped with spraying systems enable precise and targeted application of fertilizers, pesticides, and other agrochemicals. The integration of IoT allows for real-time data collection on crop conditions, pest infestations, and disease outbreaks. This data can be analyzed and processed to create application maps, guiding the UAVs to spray only the affected areas, minimizing chemical usage, and reducing the risk of over-application.

CROP SPRAYING WITH UAVS AND IOT	Pesticide danger to human Eliminated	MANAGEABLE EFFICIENT PRODUCTIVE PRECISE INEXPENSIVE
	Everywhere spray reaches	
	Time Saving	
	Recurring cost saving heavily	
	Easily scalable	
	Less harmful to soil	

Figure 7.3 Benefits of using UAVs. Make farming more profitable. Anybody can do. Help to transform farming from traditional to industrial.

7.6.2 Site-Specific Treatment

By utilizing UAVs and IoT, farmers can implement site-specific treatment strategies based on the information gathered from sensors and remote monitoring. By identifying variations in crop health, weed growth, or pest populations, UAVs can deliver the appropriate treatment to specific areas of the field, optimizing the effectiveness of the agrochemicals while reducing their overall use.

7.6.3 Reduced Environmental Impact

Crop spraying with UAVs and IoT enables farmers to minimize environmental impact. With precise application and targeted spraying, UAVs can reduce chemical drift and runoff, minimizing the risk of contamination in water bodies and neighboring areas. By minimizing chemical usage, UAVs contribute to sustainable agricultural practices and promote environmental stewardship.

7.6.4 Safety and Accessibility

UAVs equipped with spraying systems enhance safety by reducing human exposure to agrochemicals. With UAVs performing the spraying, farmers can avoid direct contact with potentially hazardous substances. Additionally, UAVs can access difficult-to-reach or hazardous areas, such as steep terrain or fields with obstacles, where traditional ground-based spraying methods may be challenging or risky.

7.6.5 Scalability and Adaptability

Crop spraying with UAVs and IoT is scalable and adaptable to various field sizes and crop types. UAVs can be programmed to follow predefined flight paths or operate autonomously, covering large areas efficiently. The adaptability of UAVs and IoT allows for customization and adjustment of spraying parameters based on specific crop requirements, ensuring optimal treatment for different crops and growth stages.

In conclusion, crop spraying with UAVs and IoT revolutionizes traditional spraying practices by enabling precision application, site-specific treatment, reduced environmental impact, and enhanced safety. The integration of UAVs and IoT promotes efficient and sustainable agricultural practices, contributing to improved crop health, minimized chemical usage, and increased productivity. Crop spraying with UAVs and IoT offers farmers a powerful tool to enhance their spraying operations and achieve better outcomes in crop protection.

7.7 Communication and Data Management in UAV-IoT Integration

Communication and data management play crucial roles in the successful integration of Unmanned Aerial Vehicles (UAVs) and the Internet of Things (IoT) in various applications, including agriculture, infrastructure monitoring, and disaster management. The seamless exchange of information between UAVs and IoT systems enables real-time decision-making, data analysis, and remote control of UAV operations. Here, we explore the key aspects of communication and data management in UAV-IoT integration.

7.7.1 Wireless Connectivity

UAVs rely on wireless communication technologies to establish connections with IoT systems. This typically involves using wireless protocols such as Wi-Fi, cellular networks, or dedicated communication standards like LoRaWAN or NB-IoT. Wireless connectivity enables data transmission, command execution, and real-time monitoring of UAV operations from the ground control station or IoT platform.

7.7.2 Sensor Data Acquisition

UAVs equipped with sensors, such as cameras, multispectral or hyperspectral sensors, and environmental sensors, collect vast amounts of data during their missions. Efficient data acquisition techniques, including onboard data processing and compression, enable UAVs to transmit relevant and actionable data to the IoT platform. This ensures that only necessary data is transmitted, reducing bandwidth requirements and improving overall communication efficiency.

7.7.3 Cloud-Based Data Storage

The data collected by UAVs during missions is often stored in cloud-based platforms or data centers. Cloud storage provides scalable and secure storage solutions for the large volumes of data generated by UAVs. It allows easy access to data from anywhere, facilitating data analysis, visualization, and collaboration among stakeholders.

7.7.4 Instantaneous Information

Instantaneous information streaming is necessary for prompt decision-making and the oversight of UAV operations. Through efficient communication protocols, UAVs can transmit data in real-time to the IoT platform, enabling stakeholders to monitor flight parameters, sensor data, and mission progress in real-time. Real-time data streaming facilitates immediate analysis and response to critical situations, ensuring timely interventions when required.

7.7.5 Integration with Visualization Tools

Effective data management in UAV-IoT integration involves integrating the data with visualization tools and dashboards. This allows stakeholders to interpret and visualize the collected data in a user-friendly and intuitive manner. Visualization tools enable the presentation of data in maps, charts, and graphs, facilitating comprehensive data analysis and decision-making.

7.8 Systems That Support Decisions Using Studying Data

Systems for making decisions using analysis of data play a crucial role in transforming raw data into actionable insights, enabling informed decision-making and strategic planning. In the context of UAV-IoT integration, data analytics and decision support systems are essential for processing, analyzing, and interpreting the vast amounts of data collected by UAVs and IoT devices. Here, we explore the significance of data analytics and decision support systems in this integration.

7.8.1 Data Preprocessing

Data collected from UAVs and IoT devices often require preprocessing to ensure data quality and consistency. Preprocessing techniques, such as data cleaning, normalization, and outlier detection, help identify and rectify errors or inconsistencies in the collected data. This ensures that the subsequent data analytics processes are based on accurate and reliable data.

7.8.2 Parametric Analytics

Parametric analytics entails the investigation and distillation of historical data in order to learn about past trends, patterns, and performance. By analyzing historical data collected by UAVs and IoT devices, descriptive analytics can provide valuable information about crop health, environmental conditions, and operational efficiency. These insights serve as a foundation for understanding the current state of affairs and identifying areas for improvement.

7.8.3 Prediction Analytics

Prediction analytics makes predictions and projections about future events using previous data. By applying statistical modeling, machine learning, and data mining techniques to the collected data, predictive analytics can estimate crop yields, predict disease outbreaks, or forecast weather patterns. These predictions enable farmers and stakeholders to proactively plan and take preventive measures, optimizing resource allocation and mitigating risks.

7.8.4 Prescriptive Analytics

Prescriptive analytics goes beyond predicting future outcomes and provides recommendations on optimal actions to achieve desired goals. By integrating historical data, real-time data from UAVs and IoT devices, and external factors such as market conditions, prescriptive analytics can suggest the best course of action for specific scenarios. For example, prescriptive analytics can recommend the most effective pesticide dosage or irrigation schedule based on crop conditions, weather forecasts, and regulatory requirements.

7.8.5 Decision Support Systems

Decision support systems (DSS) leverage data analytics techniques to assist decision-makers in making informed and evidence-based decisions. DSS combine data from UAVs and IoT devices with domain knowledge, models, and algorithms to provide decision-makers with actionable insights. These systems present data in a user-friendly format, such as dashboards or reports, allowing stakeholders to visualize trends, compare scenarios, and evaluate the potential impact of different decisions.

7.8.6 Optimization and Resource Allocation

Data analytics in UAV-IoT integration facilitates optimization and resource allocation. By analyzing data on crop conditions, weather patterns, and resource availability, optimization models can determine the optimal allocation of water, fertilizer, and insecticides, among other resources. These models can also optimize flight paths and mission planning for UAVs, maximizing coverage and minimizing operational costs.

7.8.7 Real-Time Monitoring and Alerts

Data analytics and decision support systems enable real-time monitoring and alerts for UAV operations. By continuously analyzing data from UAVs and IoT devices, stakeholders can monitor key performance indicators, identify anomalies or deviations from expected behavior, and receive alerts for immediate action. Real-time monitoring helps ensure that UAV operations are on track, and interventions can be made promptly when needed.

7.8.8 Continuous Improvement and Adaptation

Data analytics in UAV-IoT integration provides insights for continuous improvement and adaptation. By analyzing historical data and evaluating the outcomes of decisions and actions, stakeholders can identify areas for optimization, refine

models and algorithms, and continuously enhance operational efficiency. This iterative process allows for adaptive management strategies and fosters a data-driven approach to decision-making.

7.9 Case Studies

7.9.1 Case Study 1

SenseFly and Pix4D in Precision Agriculture SenseFly, a leading UAV manufacturer, and Pix4D, a provider of photogrammetry software, collaborated to integrate UAVs and IoT for crop monitoring and spraying. Their solution involved using SenseFly's eBee drones equipped with multispectral sensors to capture high-resolution imagery of crop fields. The data collected by the drones, including spectral information and vegetation indices, were processed using Pix4D's software to generate accurate orthomosaics and vegetation maps. These maps provided insights into crop health, nutrient deficiencies, and pest infestations. By combining UAVs and IoT connectivity, farmers could access this information in real-time through cloud-based platforms, enabling them to make data-driven decisions regarding fertilization, irrigation, and pest control. The integration of UAVs and IoT in this case study enhanced precision agriculture practices, resulting in improved crop yields and reduced environmental impact.

7.9.2 Case Study 2

DJI Agras MG-1 and DJI Agras MG-1P DJI, a renowned UAV manufacturer, developed the Agras MG-1 and Agras MG-1P drones specifically for agricultural spraying purposes. These drones are equipped with advanced spraying systems and integrated with IoT capabilities. They can be programmed to follow predefined flight paths or operate autonomously, ensuring precise and targeted spraying. The drones are equipped with sensors and communication modules that enable real-time data transmission to the ground control station or IoT platform. This connectivity allows farmers to monitor the progress of spraying operations, receive live status updates, and make adjustments if necessary. The integration of UAVs and IoT in the DJI Agras series provides farmers with efficient and reliable solutions for crop spraying, leading to improved accuracy, reduced chemical usage, and increased productivity.

7.9.3 Case Study 3

CropX and Crop-Spraying Drones CropX, an agricultural technology company, partnered with drone manufacturers to integrate UAVs and IoT in crop monitoring and spraying. Their solution involved using UAVs equipped with sensors to collect data on soil moisture levels, temperature, and nutrient content.

The data collected by the drones were transmitted in real-time to CropX's cloud-based platform through IoT connectivity. CropX's platform analyzed the data and provided farmers with insights into soil conditions, irrigation requirements, and fertilizer needs. By combining UAVs and IoT, farmers could efficiently monitor and manage their crops, optimizing resource allocation and reducing water and fertilizer wastage. This integration resulted in improved crop health, reduced costs, and increased sustainability in agriculture.

These case studies demonstrate the successful integration of UAVs and IoT in real-world scenarios for crop monitoring and spraying. By combining the capabilities of UAVs in data collection and IoT in real-time connectivity and data analysis, these solutions have revolutionized precision agriculture practices. The integration has led to improved crop health, reduced resource usage, increased productivity, and enhanced environmental sustainability. These success stories highlight the potential of UAV-IoT integration in transforming the agricultural industry and promoting efficient and sustainable farming practices.

7.10 Challenges and Future Directions

7.10.1 Regulatory and Legal Considerations for UAVs in Agriculture

The integration of UAVs and IoT in agriculture brings forth several regulatory and legal considerations that need to be addressed. These include the following.

7.10.1.1 Drone Regulations

Different nations' aviation agencies have established rules for UAV operations. UAV deployments in agriculture must adhere to a variety of rules, including those relating to flying heights, airspace limits, licencing, and pilot certifications. To ensure the safe and authorized utilization of UAVs, adhering to these rules is crucial.

7.10.1.2 Privacy and Data Protection

UAVs equipped with sensors and cameras raise concerns regarding privacy and data protection. Collecting data from private properties or individuals' personal information may conflict with privacy laws. It is crucial to establish protocols and guidelines for data collection, storage, and use to ensure compliance with privacy regulations.

7.10.1.3 Liability and Insurance

The use of UAVs in agriculture introduces potential liability issues in the event of accidents, property damage, or injury. Farmers and operators need to consider

appropriate liability insurance coverage to protect against such risks. Regulatory frameworks and insurance policies specific to UAV operations in agriculture are evolving to address these concerns.

7.10.2 Security and Privacy Concerns in UAV-IoT Systems

New security and privacy issues are brought about by the combination of UAVs and IoT, and they must be resolved.

7.10.2.1 Cybersecurity

UAVs and IoT devices are vulnerable to cyber threats, including unauthorized access, data breaches, and manipulation. Securing communication channels, data encryption, and implementing robust cybersecurity measures are critical to protect UAV-IoT systems from malicious activities.

7.10.2.2 Data Privacy

UAVs and IoT devices collect and transmit sensitive data about crops, farms, and operations. Safeguarding this data from unauthorized access and ensuring compliance with data protection regulations is essential. Implementing privacy controls, data anonymization techniques, and secure data storage are necessary to maintain data privacy.

7.10.2.3 System Integrity

Ensuring the integrity of UAV-IoT systems is crucial to prevent unauthorized modifications or disruptions. Measures such as firmware/software updates, system monitoring, and access controls must be implemented to protect against system tampering or malicious interference.

7.10.3 Emerging Technologies and Future Trends in UAV-Based Crop Monitoring and Spraying

The integration of UAVs and IoT in crop monitoring and spraying is an area of ongoing development. Some emerging technologies and future trends include the following.

7.10.3.1 Advanced Sensors and Imaging

UAVs will continue to benefit from advancements in sensor technology, enabling more precise and detailed data collection. High-resolution imaging, hyperspectral

sensors, and thermal cameras will provide valuable insights into crop health, nutrient levels, and pest infestations.

7.10.3.2 *AI and ML*

Algorithms for AI and machine learning will become more and more crucial for UAV-IoT integration. Technologies can analyze large datasets collected by UAVs and IoT devices to detect patterns, predict crop yields, optimize spraying strategies, and provide decision support to farmers.

7.10.3.3 *Autonomous UAVs*

The development of autonomous UAVs will further enhance efficiency and scalability in crop monitoring and spraying. Autonomous UAVs can operate without direct human intervention, following pre-programmed flight paths and conducting missions based on real-time data and analysis.

7.10.3.4 *Integration with Agricultural Management Systems*

UAV-IoT systems will become more integrated with existing agricultural management systems, such as farm management software and machinery. Seamless integration will enable data exchange and interoperability, streamlining workflows and facilitating decision-making across different agricultural processes.

7.10.3.5 *Regulatory Frameworks and Standards*

As the adoption of UAVs in agriculture continues to grow, regulatory frameworks and industry standards specific to UAV-IoT integration will evolve. Clear guidelines and standards will ensure safe and responsible operations, promote interoperability, and address concerns related to privacy, security, and environmental impact (Figure 7.4).

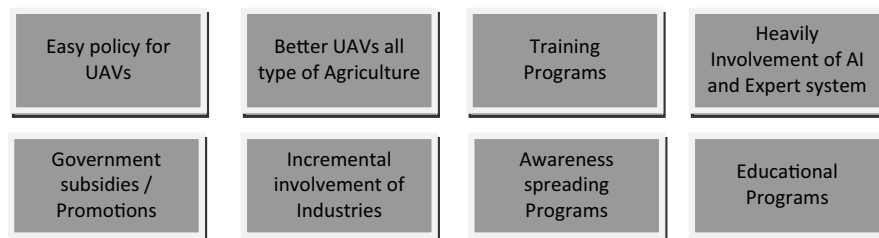


Figure 7.4 Future brightening key points, to be addressed, to be taken care, by the farmers, governments, educational and government stakeholders, all together.

Addressing these challenges and embracing emerging technologies and future trends will pave the way for the widespread adoption and optimization of UAV-IoT integration in crop monitoring and spraying, leading to increased efficiency, productivity, and sustainability in agriculture.

7.11 Conclusion

7.11.1 Recap of Key Findings and Contributions

In this chapter, we explored the integration Combining of (IoT) with UAVs, for crop monitoring and spraying. We discussed the importance of crop monitoring and spraying in modern agriculture and highlighted the potential benefits and challenges of using UAVs and IoT in crop management. We delved into the role of UAVs and IoT in agriculture, specifically focusing on crop monitoring and spraying. We examined various aspects, including communication and data management, data analytics and decision support systems, and the potential of UAVs and IoT in enhancing agricultural practices.

7.11.2 Summary of the Potential of UAVs and IoT for Irrigation and Harvest Surveillance

The integration of UAVs and IoT in crop monitoring and irrigation offers significant potential for transforming agriculture. UAVs equipped with advanced sensors and imaging technologies enable precise and timely data collection, providing insights into crop health, nutrient deficiencies, and pest infestations. IoT connectivity allows for real-time data transmission and analysis, facilitating informed decision-making and proactive management. The combination of UAVs and IoT enhances precision agriculture practices, optimizing resource allocation, reducing chemical usage, and increasing productivity. By leveraging UAVs and IoT, farmers can improve crop yields, minimize environmental impact, and achieve sustainable agricultural practices.

7.11.3 Future Prospects and Recommendations for Further Research and Development

The field of UAV-IoT integration in agriculture holds promising prospects for future research and development. To further advance this domain, several recommendations can be made, as follows.

7.11.3.1 Standardization and Regulatory Frameworks

Continued efforts are needed to establish standardized protocols and regulatory frameworks for UAV operations in agriculture. Clear guidelines will promote safe

and responsible practices and address concerns related to privacy, security, and environmental impact.

7.11.3.2 Advanced Sensing Technologies

Further development of advanced sensors and imaging technologies will enhance the capabilities of UAVs for crop monitoring. Integration of hyperspectral imaging, thermal cameras, and other advanced sensors can provide more detailed and accurate information about crop health, nutrient levels, and pest presence.

7.11.3.3 Automation and Autonomy

Advancements in automation and autonomy will contribute to the scalability and efficiency of UAV operations. Research and development should focus on developing intelligent algorithms, flight planning systems, and autonomous UAVs capable of independent decision-making and collaborative operations.

7.11.3.4 Data Analytics and AI

Continued research in data analytics, artificial intelligence, and machine learning techniques will enable more sophisticated analysis of the vast amounts of data collected by UAVs and IoT devices. This will result in improved predictive models, decision support systems, and optimization algorithms for crop management.

7.11.3.5 Integration with Existing Agricultural Systems

The integration of UAV-IoT systems with existing agricultural management systems, such as farm management software and machinery, should be further explored. Seamless data exchange and interoperability will streamline workflows, facilitate decision-making, and enhance overall farm operations.

7.11.3.6 Environmental Impact Assessment

Future research should focus on evaluating and mitigating the environmental impact of UAV operations in agriculture. Assessing the energy efficiency, carbon footprint, and ecological consequences of UAVs and IoT systems will contribute to sustainable farming practices.

In conclusion, the integration of UAVs and IoT for crop monitoring and spraying presents immense potential for revolutionizing agriculture. The combination of UAVs' data collection capabilities and IoT's real-time connectivity and data analytics opens up new possibilities for precision agriculture, resource optimization, and sustainable farming practices. Continued research, development,

and collaboration across academia, industry, and regulatory bodies will further unlock the potential of UAV-IoT integration, contributing to the advancement of agriculture and addressing the challenges faced by the industry.

References

1. Saha, A. K., Saha, J., Ray, R., Sircar, S., Dutta, S., Chattopadhyay, S. P., & Saha, H. N. (2018, January). IOT-based drone for improvement of crop quality in agricultural field. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 612–615). IEEE.
2. Boursianis, A. D., Papadopoulou, M. S., Diamantoulakis, P., Liopa-Tsakalidi, A., Barouchas, P., Salahas, G., ... & Goudos, S. K. (2022). Internet of things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: A comprehensive review. *Internet of Things*, 18, 100187.
3. Singh, P. K., & Sharma, A. (2022). An intelligent WSN-UAV-based IoT framework for precision agriculture application. *Computers and Electrical Engineering*, 100, 107912.
4. Maddikunta, P. K. R., Hakak, S., Alazab, M., Bhattacharya, S., Gadekallu, T. R., Khan, W. Z., & Pham, Q. V. (2021). Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges. *IEEE Sensors Journal*, 21(16), 17608–17619.
5. Bhuvaneshwari, C., Saranyadevi, G., Vani, R., & Manjunathan, A. (2021, February). Development of high yield farming using IoT based UAV. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1055, No. 1, p. 012007). IOP Publishing.
6. Velusamy, P., Rajendran, S., Mahendran, R. K., Naseer, S., Shafiq, M., & Choi, J. G. (2021). Unmanned aerial vehicles (UAV) in precision agriculture: Applications and challenges. *Energies*, 15(1), 217.
7. Wang, L., Huang, X., Li, W., Yan, K., Han, Y., Zhang, Y., ... & Lan, Y. (2022). Progress in agricultural unmanned aerial vehicles (UAVs) applied in China and prospects for Poland. *Agriculture*, 12(3), 397.

Chapter 8

Health-Tracking System through the Application of IoT

Kaushik Banerjee and Sudipta Adhikary

School of Law, Brainware University, Barasat, Kolkata, West Bengal, India

8.1 Introduction

There has been rapid progress in the field of wireless networks and automation during the 20th century [1], which seems to be riding a significant wave of change in the next several decades. Accessing services and smart gadgets has never been easier than it is now that the Internet is so widely available. Over the course of several decades, automation and wireless technologies have benefited greatly from the advent of the internet of things (IoT). In many fields, from home and building automation to the development of smart cities and the provision of healthcare, the Internet of Things (IoT) holds great promise for fully capitalising on the power of networking and transforming the gadget into a revolutionary service. Therefore, a new vocabulary is created as a means of connecting machines and humans through shared language. This proposal uses a smart watch to continually monitor the patient's health data, removing the need for constant steward intervention. Smart watches use a variety of sensors to collect data about a user's health, which is then sent to the cloud for analysis. A local surgeon or patient relative is given an emergency contact in case any discrepancies are found in the sent data [2,3].

8.2 Literature Survey

The healthcare system can benefit from a variety of Internet of Things applications, according to a variety of study papers. One of the primary goals of the project is the development of a wireless monitoring system; thus, we offered a system that is linked with smart devices to facilitate wireless communication and mobility. Safeguarding a patient's health by extraction of raw data from an Android app and subsequent analysis of this data. Heart problems can be diagnosed using data gathered and analysed by considering the patient's age [1]. The Raspberry Pi 3 board and the Arduino board can be used as gateways in a wireless healthcare system, connecting it to the cloud and allowing for the collection of real-time data [4,5].

This chapter provides a comprehensive overview of the smart watch's means of communication and engagement, including how wearables can be wirelessly linked to a gateway and how this smart watch can be linked to a smartphone running a suitable Android app by means of Bluetooth low energy (BLE) [6]. Keeping tabs on someone's health status is a complicated human procedure. The smart watch's passive health monitoring has helped the wearer unknowingly avoid this ailment. One more difficult issue in embedded system is integrating the smart watch's sensors and optimising the firmware for a certain architecture [3,7]. Wearables' features, especially those that provide access to additional parameters via the sensory sensors included into smart watches, are crucial for a wide variety of uses [2].

8.3 Proposed Work

A smart watch may measure a variety of factors. In particular, the electrocardiogram (ECG), photoplethysmography (PPG), and heart rate (HR) are crucial in identifying irregular heart rhythms. Connecting the smart watch to the smartphone through an Android app is required to obtain these values [8]. The conceptual framework for this study is depicted in Figure 8.1.

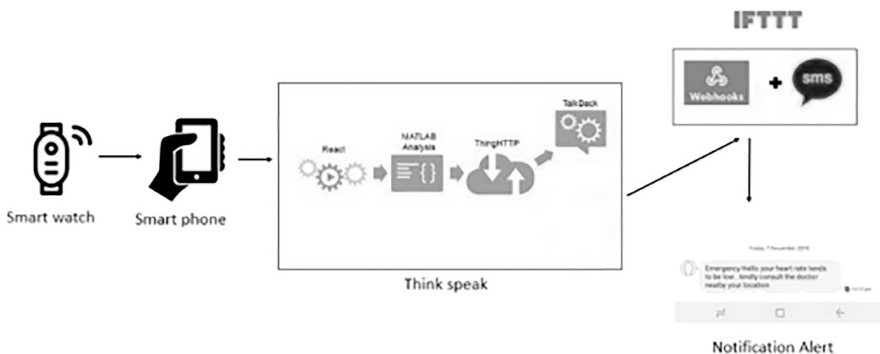


Figure 8.1 Smart health monitoring system through IoT.

8.3.1 Smart Watch

The ECG and PPG signals from a smart watch provide continual, reliable monitoring of heart rate. Figures 8.2, 8.3, and 8.5 depict the ECG and PPG signal analysis and translation findings in Figure 8.4, respectively (Table 8.1).

Bluetooth Low Energy is widely regarded as low-power wireless technology that can exchange data with other Bluetooth Low Energy gadgets. To put it simply, NFC is a protocol that allows two BLE devices to talk to one another. In order to convert the physical parameters into signals, the sensors are wired to the microcontroller. Bluetooth may be used to establish a wireless connection using the UART protocol. The antenna performs a signal scan initiated by the MCU over the UART. In order for a smart watch to go into standby mode, power must be supplied. The processing time of a smart watch and the smart watch's display both affect its standby time. In order to conserve energy, the watch's display has been removed, and in its place, a ceramic plate with two pin buttons for resetting and selecting options has been affixed. Smartphones allow users to check their battery life and have access to a wide variety of programmes. The smart watch may be tested by connecting it to a computer with a USB type C cable [9].

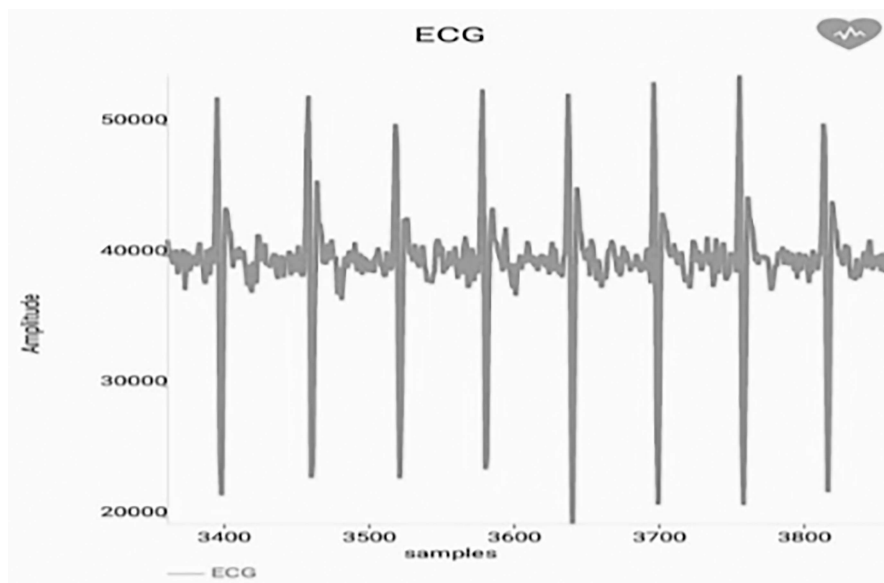


Figure 8.2 Android can explore ECG output.

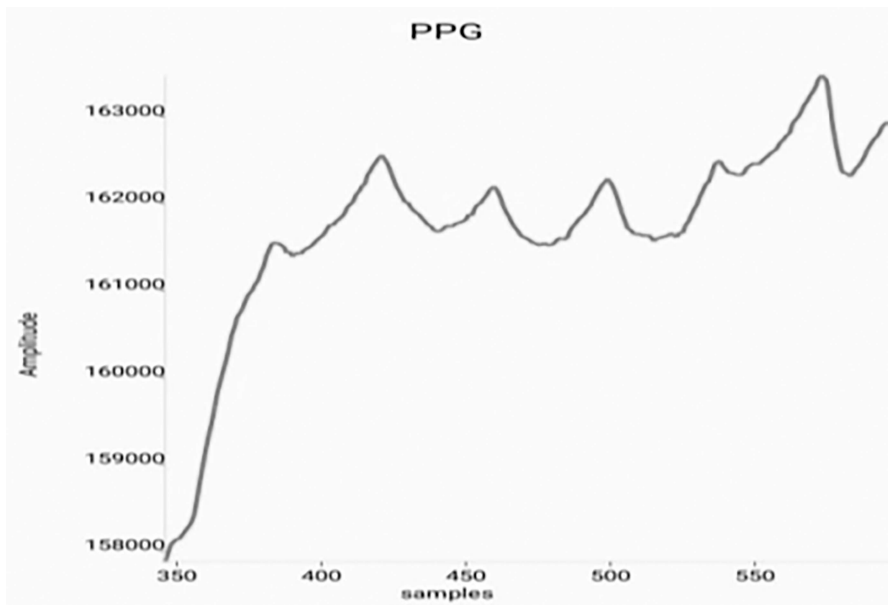


Figure 8.3 Output of PPG through Android application.

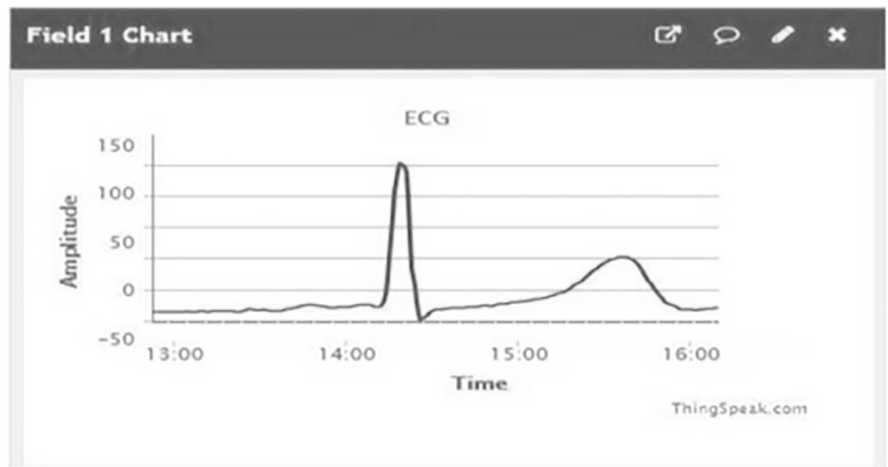


Figure 8.4 Output of ECG through Thing-speak.

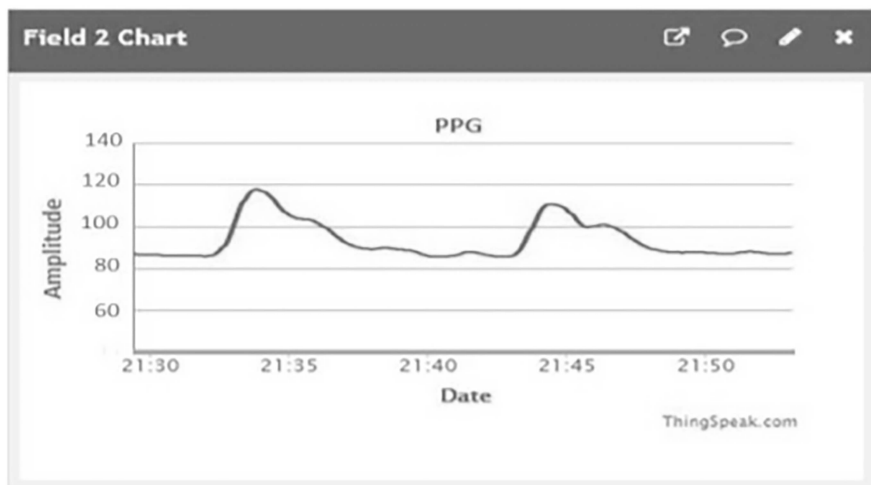


Figure 8.5 Output of PPG in Thing-speak.

Table 8.1 Application of Various Sensors

<i>Sensors</i>	<i>Applications</i>
Accelerometer, Motion	Patient motion detection, Activity and inactivity sensing detects the presence or lack of motion
Optical AFE, ECG	Heart rate monitoring, SpO2 Industrial monitoring
Temperature	Medical equipment, Environment monitoring, HVAC
Bio impedance	Photoplethysmography, Photodiode measurements
Captive sensor	Touch screen display

8.4 Smartphone

A portable electronic device has computing capabilities similar to a personal computer, but with a touch screen, cellular connectivity, and a custom operating system capable of running a variety of applications. Smartphones are used for everything from banking and business to analysis and statistics today. Here, we developed an Android app that eases the burden of constant data exchange between the wearable device and the IoT server.

Table 8.2 Mode of Communication

<i>Connected Device/ Service</i>	<i>Target Device/ Protocol</i>	<i>Mode of Communication</i>
Smart Watch	Smart Phone	(BLE-Bluetooth Low energy)
Smart Phone	Thing Speak	(Router, Mobile data)
Thing Speak	IFTTT	(Web-based service)

The real-time information in Table 8.2 is retrieved from the smart watch via an Android app's connection to it via (BLE-Bluetooth Low Energy). These real-time observations are made using a smartphone and transmitted in JSON format, which allows for easy charting. We are taking the raw data from the Android app and decoding the ECG, PPG HR data's [10].

This programme can record signals and keep a log of them. The Thing speak cloud API was integrated into this application so that data could be sent between the smart watch and Thing speak. The data is then transferred to Thing speak's analytics cloud in the cloud for additional analysis [11].

8.5 Thing Speak

The Internet of Things (IoT) is one of the cutting-edge technologies now working in tandem with medical and healthcare apps to provide accurate results. In order to simplify the process, IoT is expected to experience explosive growth in the future years. This driving technology has made it easier for relief workers to do their jobs. Data and information may be accessed via smart gadgets that are worn on the human body and continuously monitor critical factors. Several services in the cloud are available for statistical testing. As the Matlab analytics cloud, Thing Talk IoT cloud was utilised to gather, interpret, store, and analyse the data for this project. In the cloud section, we are analysing the patient's heart bit and age to determine whether the patient is in cardiac, normal, or pathological condition. The goal of this project is to upload JSON files including age, PPG, and ECG data to the cloud. The cloud then analyses these data to determine the patient's heart health. In the cloud, we use the HTTP protocol to relay aberrant alarms to the patients' neighbours and to nearby medical professionals.

8.6 IFTTT

This is a web-based service that facilitates interaction between servers. Applets are basic conditional statements that may be created with its aid. This IFTTT server



Figure 8.6 Alert received in mobile at the time of emergency.

has several applets. We're linking the Thing speak cloud with IFTTT so that when a trigger occurs in the cloud or any of the other linked platforms, these applets will appear. Web application tasks may be automated with the help of the many available automation applets [12].

8.7 Results

In this study, we analysed in depth the electrocardiogram data we received from our smart watches so that we might receive an emergency notification on our phones if our heart rates showed any signs of being abnormal. Whether the person is healthy or not is a simple matter to ascertain. If the specified IFTTT trigger fails, I have implemented an algorithm to determine what constitutes a normal and abnormal heart rate. As seen in Figure 8.6, this will send an urgent message to the patient's family.

8.8 Conclusion

This set up allows for constant tracking of our heart rates. We are extracting heart rate from ECG and PPG data collected by that smart watch. Using the patient's age and heart rate, we may make an educated guess about their heart health. Warnings were sent to the patient's family or a nearby physician if they showed signs of an unusual heart rate or other heart disease risk factors. This improves the system's adaptability.

References

1. Shah, M. H., Khan, S., Sidek, K. A., Kazmi, S. A., & Kadir, K. A. (2015). From Measurement of Photoplethysmography Signal for Heart Rate Variability and Comparison of Two Different Age Groups.

2. Bhelkar, V., & Shedge, D. K. (1998). "From Different Types of Wearable Sensors and Health Monitoring Systems: A Survey", 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp 43–48.
3. Kamisalic, A., Fister, I. Jr., Turkanovic, M., & Karakatic, S. (2018, May). From Sensors and Functionalities of Non-Invasive Wrist Wearable Devices: A Review. doi: 10.3390/s18061714
4. Pradeep Kumar, S., Samson, V. R. R., Bharath Sai, U., Malleswara Rao, P. L. S. D., & Kedar Eswar, K. (2017). "From Smart Health Monitoring System of Patient Through IoT", International Conference on I-SMAC, pp 551–556.
5. Nishitha Reddy, A., Marks, A. M., Prabakaran, S. R. S., & Muthulakshmi, S. (2017). "From IoT Augmented Health Monitoring System", 2017 International Conference on Nextgen Electronic Technologies, pp 251–254.
6. Cirani, S., & Picone, M. (2015). From Wearable Computing for the Internet of Things. *IEEE Computer Society*, 2, 35–41.
7. Maria, A. R., Pasca, S., & Strungaru, R. (2017). "From Heart Rate Monitoring by Using Non-invasive Wearable Sensor", 6th IEEE International Conference on E-Health and Bioengineering-EHB 2017, pp 587–590.
8. Mano, L. Y., Faical, B. S., Nakamura, L. H., Gomes, P. H., Libralon, G. L., Meneguete, R. I., ... & Ueyama, J. (2016). Exploiting IoT Technologies for Enhancing Health Smart Homes through Patient Identification and Emotion Recognition. *Computer Communications*, 89, 178–190.
9. Yang, Z., Zhou, Q., Lei, L., Zheng, K., & Xiang, W. (2016). An IoT Cloud Based Wearable ECG Monitoring System for Smart Healthcare. *Journal of Medical Systems*, 40(12), 286.
10. Chen, M., Ma, Y., Song, J., Lai, C. F., & Hu, B. (2016). Smart Clothing: Connecting Human with Clouds and Big Data for Sustainable Health Monitoring. *Mobile Networks and Applications*, 21(5), 825–845.
11. Jalali, R., El-Khatib, K., & McGregor, C. (2015, February). "Smart City Architecture for Community Level Services through the Internet of Things", 18th International Conference on Intelligence in Next Generation Networks (pp. 108–113). IEEE.
12. Muhammad, G., Rahman, S. M. M., Alelaiwi, A., & Alamri, A. (2017). Smart Health Solution Integrating IoT and Cloud: A Case Study of Voice Pathology Monitoring. *IEEE Communications Magazine*, 55(1), 69–73.

Chapter 9

IoT-Enabled Financial Inclusion: Challenges, Opportunities, and Policy Implications

Khurshid Ali Ganai¹, Bilal Ahmad Pandow², and Faheem Syeed Masoodi³

¹*Higher College of Technology, Abu Dhabi, Dubai, UAE*

²*Bahrain Polytechnic, Isa Town, Bahrain*

³*Department of Computer Science, University of Kashmir, Srinagar, Jammu and Kashmir, India*

9.1 Introduction

The Internet of Things (IoT) has become a game-changing tool that can change many fields, including the financial industry. Financial inclusion made possible by the IoT has gotten much attention as a way to give disadvantaged people, especially in developing countries, access to financial services. By using the fact that IoT devices are linked to each other, people can get cheap and easy-to-use financial services no matter where they live or how much money they have.

This chapter aims to give an in-depth look at how the Internet of Things (IoT) can help people access financial services. It will focus on its challenges, possibilities, policy effects, successful applications, and future research paths. The history and importance of IoT-enabled financial inclusion are examined, focusing on how it

could help solve problems like a lack of physical infrastructure, high prices, and not having access to standard banking services.

The IoT technology lets People get around these problems and access vital financial services like payments, savings, loans, and insurance. The chapter details what financial inclusion is and how it works. It also talks about how important it is to ensure that everyone has access to, uses, and can afford financial services of good quality. Then, it introduces IoT and how it relates to financial inclusion. It explains how IoT devices, sensors, and connections can make financial transactions, data collection, and analysis more safe and efficient.

On the other hand, IoT-enabled financial inclusion is not without its problems. Infrastructure problems, problems with connection, the cost and availability of IoT devices, privacy and security worries, not knowing how to use technology, and cultural differences are all significant obstacles to broad acceptance. These problems must be carefully dealt with to ensure everyone has equal access to banking services that use IoT and to reduce possible risks. On the other hand, IoT technology opens up a lot of doors when it comes to financial equality.

The IoT can improve access to financial services, cut costs through automation and remote management, provide data-driven insights for risk assessment and personalized services, help underserved groups get micro-loans and manage risks, create new products and services, and teach people about money through digital channels.

The chapter also looks at the successful uses of IoT-enabled financial inclusion programs in different countries. It shows how the IoT has changed financial services and given underserved groups more access. Implementations like M-Pesa in Kenya, the Aadhaar Enabled Payment System in India, and IoT-based agriculture finance solutions show how IoT can help close the gap in financial inclusion. Also, the chapter talks about what IoT-enabled financial inclusion means for policy and how it affects legal issues. It stresses the need for robust regulatory systems that protect customer rights, ensure data privacy and security, support interoperability, and encourage innovation.

Policy makers need to work with stakeholders to make open rules that allow IoT technology to be used in financial services responsibly and inclusively. In the last part of the study, the goals for future research and the research agenda for IoT-enabled financial inclusion are laid out. It shows the importance of looking into new technologies, user-centered design methods, impact evaluation, policy and legal frameworks, socio-economic factors, teamwork and partnerships, and new technologies' ethical and social effects. By focusing on these study areas, we can shape a future in which IoT-enabled financial inclusion is critical in promoting equal access to financial services, fostering economic empowerment, and contributing to sustainable development.

The IoT-enabled financial inclusion has much potential to help close the financial gap and give underserved groups more power. A more inclusive and resilient economic environment can be created by taking advantage of the possibilities, dealing with the problems, and implementing inclusive policies and practices. Through this chapter, we want to help people learn more about how the Internet of Things (IoT) can help with

financial inclusion. We also want to support policymakers, financial institutions, technology providers, and researchers who want to use IoT to help with financial inclusion and drive positive social and economic change.

9.2 Background and Significance of IoT-Enabled Financial Inclusion

The background and significance of IoT-enabled financial inclusion give context and a reason to look into how IoT technology can be used to provide people who don't have as much access to financial services more of it. Financial inclusion is important because it lets people use banking, credit, insurance, and payment services that are cheap. But most of the world's population, especially in developing countries, doesn't have access to formal financial services. This makes it hard for them to save, spend, and handle risks, slows down the economy's growth.

With its ability to connect devices and collect data, the Internet of Things (IoT) has changed many businesses through real-time data tracking, automation of tasks, and advanced analytics. Using IoT technology in projects to help people access money has many benefits. IoT devices can compensate for the lack of infrastructure in some places by connecting people to banking services and making digital payments through devices like smartphones, smartwatches, and smart cards.

The IoT technology also lowers the costs of standard banking services by allowing for remote banking and digital transfers, eliminating the need for expensive offices and equipment. The data that IoT devices collect gives us useful information about people's financial habits and conditions in underserved areas. This lets us customize economic goods, make credit scoring models, and make policy decisions allowing more people to access financial services.

IoT devices also improve risk assessment and management, especially in banking and insurance services, because they provide real-time data that makes risk profiling more accurate. This drives prices fairer and gives more people and companies access to financial goods they didn't have before.

IoT-enabled financial inclusion gives people and groups more power by making it easier to access financial services, control risks, and make money. This reduces poverty, boosts economic growth, and makes society more stable.

Understanding the historical background and importance of IoT-enabled financial inclusion shows how IoT technology could change how people access money. It talks about how important it is to deal with problems, look into possibilities, and develop good plans to use the IoT's potential for open financial systems. Researchers, lawmakers, and practitioners who want to use IoT technology to improve financial inclusion and make societies more fair and inclusive need to know this information.

Despite efforts by the government, regulators, and financial institutions to promote financial inclusion through digital platforms, the research reveals that the gap persists due to various factors such as illiteracy, inadequate infrastructure, power and network issues, banking failures, excessive charges, information disparities, and data privacy concerns (Ediagbonya & Tioluwani, 2023).

It has been found that in health services, machine learning has substantial financial implications (Ali Ganai & Ahmad Pandow, 2023).

9.3 Research Objectives and Scope

The primary objectives of this research are as follows:

- To investigate the role of IoT technology in facilitating financial inclusion for underserved populations.
- To identify the opportunities and challenges associated with integrating IoT in expanding access to financial services.
- To examine the impact of IoT-enabled financial inclusion on socio-economic development, poverty reduction, and economic empowerment.
- To explore the potential of IoT-generated data for enhancing risk assessment, credit scoring, and tailored financial product development.
- To analyze the policy implications and regulatory considerations for effectively leveraging IoT in financial inclusion initiatives.
- To provide insights and recommendations for policymakers, financial institutions, and stakeholders on harnessing the benefits of IoT-enabled financial inclusion.

This study looks at how IoT technology can be used to help people get access to banking services. Looking into the different ways IoT technology can be used in financial services, such as mobile banking, digital payments, lending, insurance, and financial education.

The IoT-enabled financial inclusion programs in different parts of the world will be looked at, with both developed and developing countries taken into account, to get a full picture of different situations and difficulties. Analysis of key players' roles and points of view, such as governments, financial institutions, technology companies, and community organizations, in driving IoT-enabled financial inclusion.

Identifying and analyzing the problems and opportunities of using IoT technology to help people access financial services, such as infrastructure limits, cost, privacy, security, and digital skills. Evaluating the social and economic effects of IoT-enabled financial inclusion on people, groups, and countries, such as reducing poverty, giving people more control over their finances, and keeping society stable policy and Regulatory.

The studies have investigated the level of Fintech development in the Balkan countries, considering various influencing factors such as public policies, EU membership, and financial and digital education, and identified measures to enhance financial inclusion through Fintech and digitization of financial products based on indicators related to internet usage, bank assets, online transactions, digital payments, and account ownership (Apostu et al., 2023).

Also, studies have examined the impact of digital financial inclusion and bank competition on bank stability in Sub-Saharan Africa, finding a positive relationship between digital financial inclusion and bank stability, a negative association with non-performing loans, and a negative effect of bank competition on bank stability, suggesting the need for policymakers to prioritize digital financial literacy, enhance bank competition, and implement strategic measures to preserve bank stability (Chinoda & Kapingura, 2023). While, research reveals that digital financial inclusion exerts a notable positive impact on economic growth and also generates spatial spillover effects that benefit neighboring countries (Shen et al., 2021).

The policy effects and regulatory considerations of IoT-enabled financial inclusion include data protection, customer rights, privacy laws, and collaborative governance models. The study will use literature reviews, case studies, and data analysis to achieve these objectives. This will give academics, policymakers, and practitioners in financial inclusion and IoT technology valuable insights.

9.4 Conceptual Framework

Financial inclusion means that people and companies, especially those excluded or underserved in the past, can get and use a wide range of economic goods, services, and systems. Its goal is to make sure that everyone in society, no matter their wealth, gender, age, or where they live, has access to low-cost, safe, and easy-to-use financial tools that help them handle their money, make payments, save, borrow, invest, and protect themselves from risks.

Financial inclusion comprises several key components that enable everyone to use financial services as can be observed in Figure 9.1. Among these parts are as follows:



Figure 9.1 Conceptual framework of financial inclusion.

- I. **Access to Banking Services:** This means giving people, and companies access to basic banking services like starting and keeping a bank account, putting money in and taking it out, and making financial transactions. Digital payments and electronic transactions involve letting people and companies pay electronically through mobile wallets, online platforms, or digital payment systems. This eliminates the need for cash and makes things easier and safer.
- II. **Credit and Lending:** It means giving people and companies access to loans, financing, and other forms of credit to help them meet their financial needs, make investments, and start their own businesses.
- III. **Insurance and Risk Management:** This includes making insurance products and risk management tools easy to find and cheap so that people and companies can be protected against risks like health emergencies, damage to property, natural disasters, and business interruptions.
- IV. **Savings and investments:** Its main goal is to get people and companies to save and invest their money. To do this, it offers a variety of goods and services, like savings accounts, investment accounts, mutual funds, and other ways to invest. It gives people the information, skills, and tools they need to make good financial choices, understand financial products and services, deal with debt, budget, and plan for the future.
- V. **Consumer rights and protection:** It involves making rules and policies to protect the rights and interests of consumers in their financial dealings. This includes supporting openness, fairness, and ways to settle disagreements.

Bank branch contraction is associated with increased economic growth in secular countries. In contrast, bank branch expansion combined with more significant internet usage promotes economic development in secular countries, but high ATM supply combined with more actual internet usage hinders economic growth; furthermore, in religious countries, bank branch expansion amid a widening poverty gap leads to significant economic growth, indicating the effectiveness of financial inclusion in promoting economic development in poor religious countries, and internet usage is an essential determinant of economic growth in secular countries (Ozili et al., 2023).

Also, studies have explored the relationship between financial inclusion and financial technology (Fintech), focusing on the Association of Southeast Asian Nations (ASEAN) member countries and India, examining the contributions and potential risks of Fintech in enhancing financial inclusion, comparing the strategies and implementation between India and ASEAN, and providing policy recommendations based on the findings (Morgan, 2022).

While it has been observed that the returns of IoT firms witness considerable growth, compared to the IT industry in the same period which has undergone a downturn (Pandow et al., 2020).

Even cloud computing has been providing scalable solutions that used to be challenging to manage and took a massive chunk of companies' resources (Zameer et al., 2018).

Studies have observed the handling of financial data for different missing data scenarios in three types of AI algorithms: Deep-learning, tree-based, and rule-based models (Sachan et al., 2021).

Long short-term memory (LSTM) networks, applied to predicting directional movements in the S&P 500 constituent stocks from 1992 to 2015, outperform memory-free classification methods, with daily returns of 0.46% and a Sharpe ratio of 5.8 before transaction costs, revealing high volatility and short-term reversal return patterns as sources of profitability, while exhibiting low exposure to systematic risk (Fischer & Krauss, 2018).

Machine learning encompasses various statistical techniques, including econometric regression and neural networks, with the trade-off between computational efficiency and human interpretability being a key consideration, leading to a debate between proponents of deep learning and explainable artificial intelligence (XAI); studies have extended previous research to highlight explainability as a challenge in classic machine learning approaches and suggests avenues for future research to enhance the design and efficiency of transparent algorithms (Hoepner et al., 2021).

The healthcare sector faces significant financial fraud challenges due to the utilization of credit cards, necessitating continuous enhancements in fraud detection systems using machine learning and deep learning approaches; comparative analysis reveals that the K-Nearest Neighbor (KNN) algorithm outperforms other methods in detecting credit card fraud with an accuracy of 97.58% (Mehbodniya et al., 2021).

All of these parts work together to make a financial system that meets the different financial needs of people and businesses, helps the economy grow, reduces poverty, and gives people more social and economic power.

9.5 Relevance to Financial Inclusion

The Internet of Things (IoT) is a network of gadgets, sensors, and systems that are all linked together and can receive, share, and analyze data over the Internet. These devices, which include wearables, smart sensors, embedded systems, and connected infrastructure, make it easy to share information and communicate. This improves automation, speed, and the ability to make decisions. IoT technology is helpful for financial inclusion efforts because it can help more people access banking services and close the digital gap as can be observed in Figure 9.2.

IoT can help underserved places with few standard banking facilities linked to the Internet. IoT-enabled devices like cell phones and smart cards allow people to access banking services, make deals, and get information from far away, even in rural or remote areas. IoT makes it possible for digital payments and mobile banking options to become more popular.

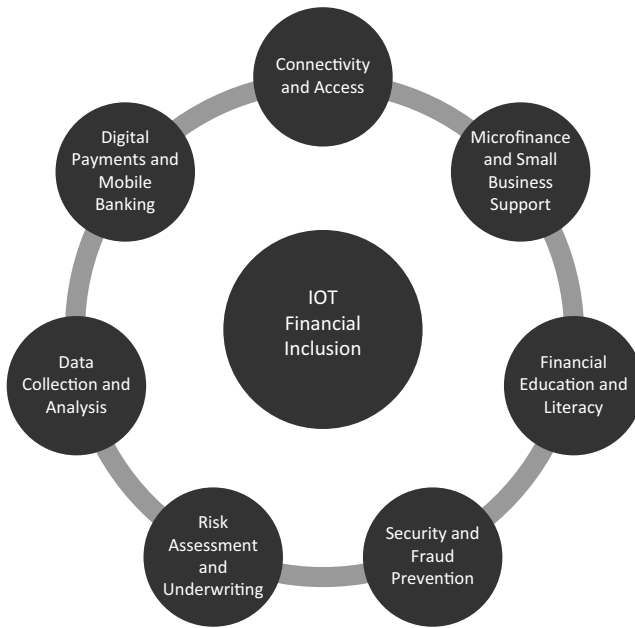


Figure 9.2 Relevance to financial inclusion.

People can make transactions, move money, and use banking services safely through IoT-connected products. This makes it less necessary to go to an actual store and makes it easier for people to get money, especially in places where it's hard to get to a bank. IoT gadgets generate a huge amount of data in real-time. This information can be used to learn important things about neglected groups' financial habits, trends, and needs. Financial institutions and policymakers can use this data to make customized economic goods and services that meet specific needs and desires and, ultimately, help more people get access to financial services.

Data from the IoT can be used to improve risk assessment and insurance, especially for people with short credit records. Real-time data from IoT sensors and devices, such as smartphone usage habits, geolocation data, and transaction history, can make credit scoring models more accurate and dynamic. This can help people who haven't been able to get banking services in the past.

Small businesses and loan programs can use IoT technology to help them. By using IoT sensors and devices, financial institutions can monitor the performance of small businesses, farming activities, and supply lines from afar and evaluate their performance. This information can help give credit, offer customized financial solutions, and reduce the risks involved with these projects. This encourages people to start their own businesses, which helps the economy grow.

IoT improves security steps and makes it easier to stop scams. With IoT-enabled systems, financial institutions can use multi-factor authentication,

biometric identification, and safe data encryption to build trust and reduce fraud risks in financial operations. Financial education and learning programs can be run with the help of IoT gadgets.

Some studies fill a literature gap by conducting an in-depth review of deep learning technology and its applications in the banking sector, serving as a comprehensive resource for banks and researchers interested in adopting deep learning and offering insights for future research and implementation (Hassani et al., 2020).

The security and privacy challenges associated with IoT implementation in the financial industry pose significant obstacles for financial services firms, requiring robust measures to protect against various forms of cyberattacks and ensure system integrity (Masoodi & Pandow, 2021).

It has been found that the interplay between financial inclusion, financial consumer protection, financial integrity, and financial stability, highlighting that effective management within the regulatory framework is crucial to ensure positive relationships among these factors and identifies areas for further research (Cull et al., 2012).

With IoT-enabled platforms, people can access educational resources, engaging tools, and personalized financial advice. This helps them make better financial choices and improve their economic well-being. Overall, putting IoT technology into financial inclusion efforts could help solve geographical and infrastructure hurdles, make it easier for people to get financial services, and use data-driven insights to make financial solutions that are more inclusive. By using the power of IoT, financial institutions, policymakers, and other players can help build economic environments that work for more people and last longer.

9.6 Challenges of IoT-Enabled Financial Inclusion

One of the most significant challenges with using IoT to help people get access to banking services is that there isn't enough infrastructure, especially in rural and remote places. IoT devices can't work smoothly if they don't have enough internet access, enough network coverage, or a stable power source. This makes it harder for underserved groups to get access to financial services.

The price of IoT products and services can make it hard for people to enter the banking system. Many people in underserved areas may not have the money to buy IoT-enabled gadgets or pay for the data plans needed to join. IoT technology's price needs to be considered if everyone is to get the same benefits from it. IoT gadgets collect and send out much information about people and their finances.

Concerns about privacy and security are raised when private information is collected, stored, and shared. IoT networks could be vulnerable to unauthorized access, data breaches, and identity theft if there aren't enough security measures and holes in them. This would hurt trust in banking systems.

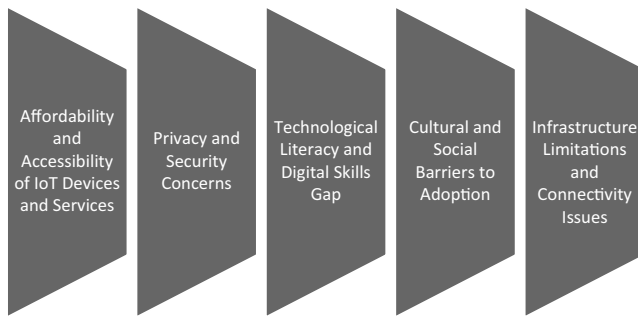


Figure 9.3 Challenges of IoT-enabled financial inclusion.

To fully benefit from IoT-enabled financial inclusion, addressing the digital skills gap and providing adequate training and support to individuals in disadvantaged communities who may face challenges in understanding and utilizing IoT devices is essential. Furthermore, the utilization and adaptation of IoT-enabled banking services may vary based on cultural norms, perspectives, and other social factors.

IoT solutions can be harder to accept and use if people have old ways of thinking about money, don't trust technology, or don't like change. It is essential to think about cultural and social contexts, develop open approaches to everyone, and meet each group's needs and desires.

To deal with these problems, we need a complete plan that brings together governments, banking institutions, technology companies, and community organizations, among other groups. Also, as mentioned in Figure 9.3, the strategies like improving infrastructure, lowering the cost of IoT devices, improving data privacy and security, offering digital literacy programs, and promoting inclusive and culturally sensitive approaches can help IoT-enabled financial inclusion overcome its challenges and reach its full transformative potential.

9.7 Opportunities for IoT-Enabled Financial Inclusion

The IoT technology can make it easier for more people to get banking services by getting around geographical barriers and connecting places that aren't getting enough help and various opportunities for IoT-enabled financial inclusion are enlisted in Figure 9.4. IoT-enabled devices, like cell phones and smart cards, can make online banking, digital payments, and access to financial information easier. This lets people in remote and rural areas participate in the official financial system.

The IoT technology can lower the costs of running businesses that provide banking services. Financial institutions can use IoT devices and platforms to reduce the need for real infrastructure like brick-and-mortar branches and offer services online. This ability to grow can help reach more people for less money, making banking services more cheap and long-lasting.

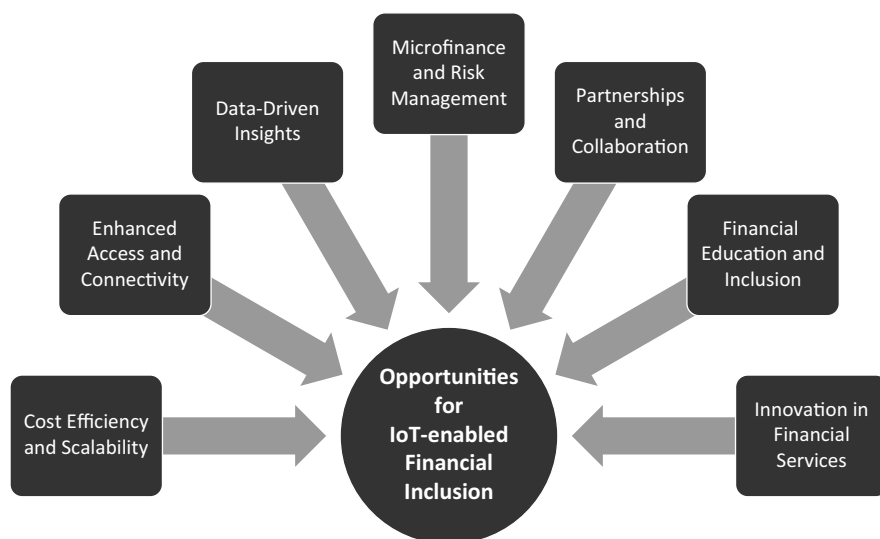


Figure 9.4 Opportunities for IoT-enabled financial inclusion.

Data from the IoT gives us important information about how people in poor areas handle their money and what they need. By looking at this data, financial institutions can learn more about their customers' tastes, risks, and reliability. This lets them make more personalized economic goods and services. Insights from data can also help guide policy choices and actions that aim to improve financial inclusion.

IoT technology can help with lending projects and make it easier for financial services companies to control risks. IoT sensors and devices can give real-time information about microbusinesses, farming activities, supply lines, and insurance claims. This makes it possible to measure and reduce risks more accurately. This can lead to the creation of new financial goods, more people getting access to microfinance, and stronger small businesses.

The IoT allows new financial services and business models to be created. IoT-based payment systems, like mobile wallets and wireless payments, can be used to make easy and safe transactions. IoT-enabled credit score models can make getting loans easier for people with short credit records. These innovations can give underserved groups more power, help more people access money, and help the economy grow.

IoT devices and platforms can offer financial education and literacy programs to people who might not have access to standard learning tools. IoT apps can give personalized financial advice, planning tools, and real-time financial information. This helps people learn more about money and gives them the power to make smart financial choices.

For financial inclusion to be made possible through IoT, many different groups, such as states, financial institutions, technology companies, and

community organizations, must work together. These partnerships can use each other's skills and resources to create and implement comprehensive solutions that meet the unique problems of financial inclusion.

By taking advantage of the possibilities offered by the Internet of Things (IoT), underserved groups can access a wider range of banking services, build economic resilience, and take a more active role in the global economy. Players must take advantage of these chances and work well together to get the most out of IoT-enabled financial inclusion.

9.8 Successful Implementations of IoT-Enabled Financial Inclusion Initiatives

Successful implementations of IoT-enabled financial inclusion programs have shown how powerful it can be to use IoT technology to increase access to financial services, especially for people who don't have enough of them. By using IoT devices, connectivity, and data-driven insights to give people and communities cheap, safe, and easy-to-use financial tools, these efforts have helped close the financial inclusion gap.

Initiatives for financial inclusion that use the Internet of Things (IoT) have been implemented in many countries and areas, showing both creative solutions and good results. These changes have not only made it easier for underserved people to use standard banking services, but they have also made it possible for them to use new financial goods and services better suited to their needs.

By using IoT technology, these projects have fixed infrastructure problems, gotten around geographical problems, and brought banking services to rural and underserved areas. IoT-enabled devices like smartphones, wearables, and smart cards have opened doors to banking services, digital payments, and other financial tools, giving people the power to handle their finances, make deals, and protect themselves from risks.

Also, successful projects have used real-time data collection and analysis from IoT devices to learn about how people in underserved areas handle their money, what they like, and what they need. Based on data, this method has made it easier to create customized financial goods, credit scoring models, and focused interventions to help more people access financial services. IoT-enabled financial inclusion projects help more than just those who participate in them.

These projects have helped improve the economy and society by lowering poverty, boosting economic growth, and making finances more stable. IoT-enabled financial inclusion has made it easier for people and companies to save, invest, spread their spending, and get insurance. This has helped people and groups build up their economic resilience and take a more active role in the economy.

Some studies have examined the role of IoT in digital financial inclusion, addressing the barriers faced by unbanked individuals and the potential benefits of

combining online financial tools, such as smartphone remittances via IoT, with psychological tools like financial education, based on a study of 120 respondents from the National Capital Region, which identifies seven significant factors including IoT awareness, financial service awareness, usability, benefits, trust, security, privacy, and accessibility influencing the role of IoT in digital financial inclusion (Kumar & Anjali, 2023).

By looking at these case studies, lawmakers, banking institutions, and other interested parties can learn about best practices, lessons learned, and possible areas for future growth. In the end, the lessons learned from successful implementations will help advance the field of IoT-enabled financial inclusion and guide future efforts to increase access to financial services, promote inclusive economic growth, and improve the overall well-being of individuals and communities.

- I. **M-Pesa (Kenya):** M-Pesa is a widely recognized example of a successful IoT-enabled financial inclusion initiative. It is a mobile phone-based money transfer and payment system that has transformed financial services in Kenya. Through M-Pesa, individuals can securely send and receive money, make payments, and access other financial services using their mobile phones. This initiative has significantly expanded access to financial services, particularly in rural areas, and has increased financial inclusion in the country.
- II. **Aadhaar Enabled Payment System (India):** India's Aadhaar Enabled Payment System (AEPS) is an IoT-enabled initiative that leverages biometric authentication to facilitate secure and convenient financial transactions. AEPS enables individuals to access their bank accounts, make payments, and receive government subsidies using their Aadhaar biometric identification. This initiative has improved financial access for millions of unbanked individuals in India, fostering financial inclusion and reducing reliance on cash transactions.
- III. **Smart Grids for Pay-as-You-Go Solar Energy (Various countries):** IoT-enabled smart grids provide pay-as-you-go solar energy solutions to off-grid communities in several developing countries. These systems utilize IoT sensors and devices to monitor energy usage, collect payments, and remotely activate or deactivate energy supply. By combining IoT technology with innovative financing models, such as microfinance, these initiatives have made clean energy affordable and accessible to underserved populations, improving their quality of life and promoting financial inclusion.
- IV. **IoT-based Agricultural Finance (Various countries):** IoT-enabled solutions have been implemented in the agricultural sector to facilitate access to finance for smallholder farmers. IoT sensors and devices collect real-time data on weather conditions, soil moisture levels, and crop health. This data is then analyzed to assess risks and provide farmers with customized agricultural financing options, including crop insurance, credit, and inputs.

These IoT-based agricultural finance initiatives have helped farmers mitigate risks, increase productivity, and improve their financial well-being.

- V. **IoT-enabled Microinsurance (Various countries):** Microinsurance initiatives that leverage IoT technology have successfully provided affordable insurance coverage to underserved populations. IoT sensors collect data on insured assets, such as livestock or crops, and monitor risks like weather conditions or disease outbreaks. This real-time data enables efficient claims processing and risk management, making microinsurance more accessible and viable for low-income individuals and small businesses.

These successful implementations demonstrate the potential of IoT-enabled financial inclusion initiatives to overcome barriers and extend access to financial services to underserved populations. By innovatively leveraging IoT technology, these initiatives have contributed to poverty reduction, economic empowerment, and improved livelihoods for individuals and communities. They serve as valuable examples for policymakers, financial institutions, and stakeholders seeking to implement similar initiatives in their regions.

9.9 Policy Implications and Regulatory Considerations

Policy implications and regulatory considerations are crucial in shaping the implementation and effectiveness of IoT-enabled financial inclusion initiatives. As IoT technology continues transforming the economic landscape, policymakers and regulators face creating a conducive environment that ensures IoT's safe, secure, and responsible use in financial services.

Integrating IoT devices, connectivity, and data-driven insights in financial inclusion initiatives introduces new opportunities and challenges that require thoughtful policy frameworks. These policies aim to balance fostering innovation and ensuring consumer protection, data privacy, and systemic stability.

The studies explore the expansion of mobile technologies in promoting digital financial inclusion, enabling access to basic banking services, savings, lending, insurance, and other financial services for the unbanked population, who face barriers due to poverty and lack of formal banking services, highlighting the importance of bridging the gaps between physical, digital, and psychological aspects of money through digital financial tools and financial education to uplift the unbanked and break the cycle of poverty (Chu, 2018).

However, it has been observed that financial exclusion hampers the access of the poor and disadvantaged to formal financial systems, leading the unbanked and underbanked to rely on costly alternative channels; the limitations of banks in catering to their needs due to regulations, legacy systems, and organizational challenges have opened doors for Fintech firms, while the proliferation of mobile phones, technological infrastructure, big data utilization, financial education, and

technological literacy have fueled financial innovation and deepened financial services (Agarwal et al., 2020).

Policy implications encompass many areas, including data governance, consumer rights, market competition, interoperability, standardization, and cybersecurity. Policymakers must establish clear guidelines and regulations to govern the collection, storage, and use of financial and personal data generated by IoT devices. They must also promote transparency, fair practices, and accountability among financial service providers leveraging IoT technology.

Besides, cross-sector collaboration among regulators, financial institutions, technology providers, and consumer advocacy groups is essential to develop comprehensive policies and regulatory frameworks. It is important to engage stakeholders in ongoing dialog to understand the evolving nature of IoT technology, address emerging risks, and adapt regulatory approaches accordingly.

- I. **Regulatory Frameworks:** Governments must establish clear and robust regulatory frameworks that address the unique challenges and risks associated with IoT-enabled financial inclusion. These frameworks should encompass data protection, privacy, cybersecurity, interoperability, consumer rights, and ethical considerations. Regulators should collaborate with stakeholders to develop flexible and adaptive regulations that foster innovation while ensuring consumer protection and system integrity.
- II. **Data Privacy and Security:** IoT-enabled financial inclusion initiatives involve collecting and processing sensitive personal and financial data. Policymakers and regulators must prioritize data privacy and security, implementing measures to safeguard against unauthorized access, data breaches, and misuse of personal information. Organizations should comply with stringent data protection standards, ensuring transparency, informed consent, and secure data storage and transmission.
- III. **Interoperability and Standards:** Promoting interoperability and setting common standards across IoT devices, platforms, and systems is crucial for seamless integration and compatibility. Policymakers should encourage collaboration among stakeholders to develop interoperable solutions that allow individuals to access financial services across different devices and networks. Setting industry-wide standards can enhance competition, innovation, and consumer trust in IoT-enabled financial inclusion services.
- IV. **Digital Identity and KYC:** Developing robust digital identity systems and Know Your Customer (KYC) processes are essential for IoT-enabled financial inclusion. Governments can play a key role in establishing reliable and secure digital identification mechanisms, such as biometric authentication, to verify individuals' identities and enable access to financial services. Policies should promote interoperability and trust among different digital identity systems while ensuring privacy and protection against identity theft.

- V. **Consumer Protection:** Policymakers should prioritize consumer protection in IoT-enabled financial services. This includes ensuring pricing, terms, and conditions transparency, promoting fair practices, and establishing mechanisms for dispute resolution and complaint handling. Regulators should monitor and enforce compliance with consumer protection regulations, taking proactive measures to educate consumers about their rights and responsibilities in using IoT-enabled financial services.
- VI. **Digital Literacy and Skills Development:** Governments and stakeholders should invest in digital literacy programs to enhance individuals' understanding and skills in using IoT-enabled financial services. These programs should target underserved populations, providing training on IoT devices, digital transactions, data security, and privacy. Empowering individuals with the necessary digital skills and knowledge is crucial to ensure their effective participation in IoT-enabled financial inclusion initiatives.
- VII. **Public-Private Partnerships:** Policymakers should foster public-private partnerships to drive IoT-enabled financial inclusion. Collaboration among governments, financial institutions, technology providers, and community organizations can leverage expertise, resources, and knowledge-sharing to develop inclusive and sustainable solutions. Policymakers should create an enabling environment encouraging collaboration and incentivizing private sector participation in IoT-enabled financial inclusion initiatives.

By addressing these policy implications and regulatory considerations, policymakers can create an enabling environment that promotes IoT technology's responsible and inclusive deployment in financial inclusion. This will help unlock the full potential of IoT, expand access to financial services, and contribute to economic growth and social development. Continuous monitoring, evaluation, and adaptation of policies and regulations are necessary to keep pace with the evolving landscape of IoT-enabled financial services.

9.10 Future Directions and Research Agenda

Future research should explore advancements in IoT technology that can further enhance financial inclusion. This includes investigating the potential of emerging technologies like 5G, edge computing, and blockchain in strengthening IoT-enabled financial services. Research can also explore the integration of IoT with other emerging technologies, such as artificial intelligence and machine learning, to develop more personalized and efficient financial solutions.

Understanding underserved populations' needs, preferences, and challenges is crucial for developing inclusive and user-friendly IoT applications and devices.

Research can explore human-centered design methodologies and user experience evaluation techniques to ensure IoT solutions are accessible, intuitive, and culturally appropriate.

There is a need for comprehensive research to evaluate the impact of IoT-enabled financial inclusion initiatives. Assessing these initiatives' effectiveness, efficiency, and sustainability can provide insights into their long-term benefits and potential challenges. Research can employ mixed-methods approaches, including qualitative and quantitative analysis, to measure the social, economic, and developmental impacts of IoT-enabled financial inclusion on individuals, communities, and economies.

As IoT-enabled financial inclusion continues to evolve, research should examine the effectiveness and adaptability of existing policies and regulations. Studying the policy implications, regulatory challenges, and legal frameworks surrounding IoT-enabled financial services can inform policymakers in developing practical and forward-thinking rules that promote innovation, protect consumers, and ensure the ethical use of IoT technology.

Investigating the role of cultural norms, gender dynamics, social networks, and community engagement can provide valuable insights for designing inclusive IoT solutions. Research can also explore the role of IoT in addressing broader development goals, such as poverty reduction, gender equality, and sustainable development.

Research should study the dynamics of collaboration and partnerships among stakeholders in IoT-enabled financial inclusion initiatives. Understanding the factors that facilitate or hinder successful collaborations can guide policymakers and practitioners in fostering effective partnerships between governments, financial institutions, technology providers, and community organizations. Research can also explore innovative funding models and business models that incentivize collaboration and sustainability in IoT-enabled financial inclusion initiatives.

As IoT technology becomes increasingly integrated into financial services, research should address the ethical and social implications of IoT-enabled financial inclusion. This includes exploring data ownership, consent, privacy, and algorithmic bias issues. Understanding the ethical considerations and potential social impacts of IoT-enabled financial services can inform the development of responsible and inclusive practices.

By focusing on these future directions and research agenda, we can deepen our understanding of IoT-enabled financial inclusion, address its challenges, and leverage its potential to promote equitable access to financial services, foster economic empowerment, and contribute to sustainable development. Continued research and collaboration are essential for shaping the future of IoT-enabled financial inclusion in a way that benefits all individuals and communities, leaving no one behind.

9.11 Conclusion

IoT-enabled financial inclusion holds immense potential to transform the way individuals and communities access and engage with financial services. By leveraging IoT technology, financial inclusion can be extended to underserved populations, empowering them to participate in the formal financial system, build economic resilience, and improve their overall well-being.

This chapter has explored the background, challenges, opportunities, policy implications, and successful implementations of IoT-enabled financial inclusion initiatives. We have discussed the importance of addressing infrastructure limitations, affordability, privacy and security concerns, technological literacy, and cultural barriers to ensure inclusive and equitable access to IoT-enabled financial services.

Also, we have highlighted the significant opportunities that IoT technology offers in expanding access, reducing costs, generating data-driven insights, fostering innovation, and promoting financial education. Successful implementations in various countries have demonstrated the positive impact of IoT-enabled financial inclusion, such as M-Pesa in Kenya, Aadhaar Enabled Payment System in India, and IoT-based solutions in agriculture and microinsurance.

However, it is crucial to acknowledge that realizing the full potential of IoT-enabled financial inclusion requires concerted efforts from policymakers, regulators, financial institutions, technology providers, and community organizations. Collaboration, flexible regulatory frameworks, data privacy and security measures, digital literacy programs, and user-centric design approaches are vital in creating an enabling environment for inclusive and sustainable IoT-enabled financial services.

As we look to the future, we must continue research in emerging technologies, user-centric design, impact evaluation, policy and regulation, socio-economic factors, collaboration and partnerships, and ethical and social implications. By addressing these research areas, we can shape the future of IoT-enabled financial inclusion, drive innovation, and ensure that the benefits of IoT technology are harnessed to promote financial inclusion and contribute to broader social and economic development goals.

In conclusion, IoT-enabled financial inclusion has the power to bridge the digital divide, empower underserved populations, and create a more inclusive and resilient financial ecosystem. By leveraging the opportunities, addressing the challenges, and implementing inclusive policies and practices, we can build a future where every individual has access to affordable, secure, and tailored financial services, fostering economic growth and enhancing the overall well-being of societies.

References

- Agarwal, S., Qian, W., & Tan, R. (2020). Financial Inclusion and Financial Technology. In *Household Finance* (pp. 307–346). Springer Nature. 10.1007/978-981-15-5526-8_9

- Ali Ganai, K., & Ahmad Pandow, B. (2023). Understanding Financial Impact of Machine and Deep Learning in Healthcare: An Analysis. In *Applications of Machine Learning and Deep Learning on Biological Data* (pp. 41–56). Auerbach Publications. 10.1201/9781003328780-3
- Apostu, S. A., Panait, M., Vasile, V., Sharma, G. D., & Vasile, R. (2023). FinTechs and Financial Inclusion—Balkan Experience: Digital Perspectives on Financial Markets. *The Electronic Journal of Information Systems in Developing Countries*, 89(2). 10.1002/isd2.12257
- Chinoda, T., & Kapingura, F. M. (2023). The Impact of Digital Financial Inclusion and Bank Competition on Bank Stability in Sub-Saharan Africa. *Economies*, 11(1). 10.3390/economies11010015
- Chu, A. B. (2018). Mobile Technology and Financial Inclusion. In *Handbook of Blockchain, Digital Finance, and Inclusion* (Vol. 1, pp. 131–144). Academic Press. 10.1016/B978-0-12-810441-5.00006-3
- Cull, R., Demirgüç-Kunt, A., & Lyman, T. (2012). Financial Inclusion and Stability: What Does Research Show? *CGAP Brief, May* (2008), 1–4. <https://www.cgap.org/research/publication/financial-inclusion-and-stability-what-does-research-show>
- Ediagbonya, V., & Tioluwani, C. (2023). The Role of Fintech in Driving Financial Inclusion in Developing and Emerging Markets: Issues, Challenges and Prospects. *Technological Sustainability*, 2(1), 100–119. 10.1108/techs-10-2021-0017
- Fischer, T., & Krauss, C. (2018). Deep Learning with Long Short-Term Memory Networks for Financial Market Predictions. *European Journal of Operational Research*, 270(2), 654–669. 10.1016/j.ejor.2017.11.054
- Hassani, H., Huang, X., Silva, E., & Ghodsi, M. (2020). Deep Learning and Implementations in Banking. *Annals of Data Science*, 7(3), 433–446. 10.1007/s40745-020-00300-1
- Hoepner, A. G. F., McMillan, D., Vivian, A., & Wese Simen, C. (2021). Significance, Relevance and Explainability in the Machine Learning Age: An Econometrics and Financial Data Science Perspective. *European Journal of Finance*, 27(1–2), 1–7. 10.1080/1351847X.2020.1847725
- Kumar, J., & Anjali. (2023). Role of the Internet of Things (IoT) in Digital Financial Inclusion. In *IoT Based Smart Applications* (pp. 363–373). Springer Nature. 10.1007/978-3-031-04524-0_21
- Masoodi, F., & Pandow, B. A. (2021). Internet of Things: Financial Perspective and Its Associated Security Concerns. *International Journal of Electronic Finance*, 10(3), 145–158. 10.1504/IJEF.2021.115644
- Mehbodniya, A., Alam, I., Pande, S., Neware, R., Rane, K. P., Shabaz, M., & Madhavan, M. V. (2021). Financial Fraud Detection in Healthcare Using Machine Learning and Deep Learning Techniques. *Security and Communication Networks*, 2021. 10.1155/2021/9293877
- Morgan, P. J. (2022). Fintech and Financial Inclusion in Southeast Asia and India. *Asian Economic Policy Review*, 17(2), 183–208. 10.1111/aepr.12386
- Ozili, P. K., Lay, S. H., & Syed, A. A. (2023). Impact of Financial Inclusion on Economic Growth in Secular and Religious Countries. *Journal of Financial Regulation and Compliance*. 10.1108/JFRC-08-2022-0093
- Pandow, B. A., Bamhdi, A. M., & Masoodi, F. (2020). Internet of Things: Financial Perspective and Associated Security Concerns. *International Journal of Computer Theory and Engineering*, 12(5), 123–127. 10.7763/ijcte.2020.v12.1276

- Sachan, S., Almaghrabi, F., Yang, J. B., & Xu, D. L. (2021). Evidential Reasoning for Preprocessing Uncertain Categorical Data for Trustworthy Decisions: An Application on Healthcare and Finance. *Expert Systems with Applications*, 185(December 2020), 115597. 10.1016/j.eswa.2021.115597
- Shen, Y., Hu, W., & Hueng, C. J. (2021). Digital Financial Inclusion and Economic Growth: A Cross-Country Study. *Procedia Computer Science*, 187, 218–223. 10.1016/j.procs.2021.04.054
- Zameer, A., Pandow, B. A., & Singh, B. (2018). Economic Hurdle for Implementation of Cloud Computing in Higher Education in Sultanate of Oman. *2017 International Conference on Infocom Technologies and Unmanned Systems: Trends and Future Directions, ICTUS 2017, 2018-January*, 2011–2014. 10.1109/ICTUS.2017.8286007

Chapter 10

Enhancing the Security of Pregnancy Health Data Transmission through Homomorphic Encryption: An Advanced Model

Mohammad Mobarak Hossain¹,
Nasim Mahmud Nayan², and
Mohammad Abdul Kashem¹

¹*Department of Computer Science and Engineering, Dhaka University of Engineering and Technology (DUET), Dhaka, Bangladesh*

²*Department of Computer Science and Engineering, University of Information Technology and Sciences (UITS), Dhaka, Bangladesh*

10.1 Introduction

In the digital age, ensuring patient privacy and data security is extremely difficult when sensitive healthcare data are collected and sent. This is crucial for prenatal health data since it contains sensitive and private information. Strong security

measures are necessary to protect such data's confidentiality and integrity. While in use and at rest, data privacy has become a significant concern in recent years [1]. A comprehensive security strategy must be implemented to ensure medical data security, including secure authentication protocols, access controls, and encryption. Another vital concern is MCPS privacy. Medical-cyber-physical systems are commonly scattered extensively across massive geographic regions to collect enormous amounts of data for data analysis and decision-making. The system makes decisions by using the data obtained in the form of sophisticated machine learning algorithms (ML). ML is widely used in different sector [2]. To ensure the data is secure, it is crucial to utilize powerful encryption techniques regularly updated [3]. Organizations should implement robust security strategies to protect their medical cyber-physical systems from unauthorized access, malicious software, data breaches, ransomware, and other threats [4]. Due to their flaws and vulnerabilities, several conventional security algorithms, including DES, SHA-1, and RC4, may need to be more effective in securing medical data. The 1970s-developed symmetric-key encryption method DES is susceptible to brute-force assaults [5]. It has been discovered that the cryptographic hash function SHA-1, which is extensively used for data integrity and authentication, has flaws that render it susceptible to collision attacks [6]. In the 1990s and the beginning of the 2000s, RC4, a famous symmetric-key stream cipher, had serious flaws that left it open to attacks. Thus, swapping out these algorithms for more sophisticated and secure standards has been advised [7]. Data breaches [8], data privacy violations [9], and malicious assaults [10] are a few of the difficulties. Traditional security algorithms are not designed to protect healthcare data, so more robust security strategies such as encryption, access control, two-factor authentication, and data analysis must be implemented [11]. One promising approach to address this challenge is homomorphic encryption, a cryptographic technique. Numerous applications of homomorphic encryption technology have been described in the literature recently [12,13], and it is a revolutionary new technology that offers private cloud storage and computing solutions. Homomorphic encryption techniques are utilized extensively in various applications to secure user data and privacy, including those in the financial, industrial, and medical sectors [14]. Sudha and his colleague [15] state, "Homomorphic encryption offers a potent method for safeguarding healthcare data privacy while facilitating secure data operations." Healthcare professionals may use homomorphic encryption to calculate and analyze encrypted prenatal health data without first decoding it, lowering the danger of hacking and illegal access. The performance of the encryption algorithms, safe transmission protocols, storage techniques, and usability must all be considered when homomorphic encryption is implemented to transfer pregnant health data. To further improve the security and efficacy of the suggested technique, it is imperative to address the shortcomings and potential holes in current approaches. This study suggests a sophisticated method for improving the security of transmitting pregnancy-related health data using homomorphic encryption. Using intelligent IoT devices for safe

data collecting, robust homomorphic encryption methods, secure transmission and storage protocols, secure data analysis and treatment, and improvements to overcome observed shortcomings are all included. The suggested advanced mode intends to maintain the security, integrity, and privacy of pregnant health data while allowing secure data analysis and treatment by integrating these elements. It also examines how to adopt and practically use the suggested strategy in real-world healthcare circumstances and possible advantages, difficulties, and prospects. The contribution of this work is as follows:

- **Comprehensive Pregnancy Data Collection:** The suggested technique utilizes Smart IoT devices to gather data on pregnancies, giving medical practitioners critical new insights into the health and well-being of pregnant women.
- **Robust Homomorphic Encryption method:** To ensure that calculations may be done on encrypted pregnant health data without decryption, the model improves the performance of the homomorphic encryption method. This protects the data privacy throughout processing and analysis.
- **Secure transmission and Storage:** The suggested technique enables the secure delivery of encrypted pregnant health data using protocols like HTTPS or SSL.

The remaining portions of the essay are organized as follows. The literature review is covered in Section 10.2, and the technique is covered in Section 10.3. Sections 10.4 and 10.5 explain the result analysis, discussion, and conclusion.

10.2 Related Work

We collect our study papers from databases like Google Scholar, Research Gate, PubMed, IEEE Explorer, etc. We need to mail the author for the draft file for a few papers. We initially collected 80 papers, and then we went through some processes like removing duplicate papers, no relevant reports and case studies, papers without encryption algorithms, or papers with flaws and vulnerabilities. Finally, we got 34 relevant papers for study. We proposed a method after studying these papers wisely and through literature studies (Figure 10.1).

This literature study examines homomorphic encryption in healthcare data security, security issues with the transmission of prenatal health data, and existing security-enhancement techniques and suggests a cutting-edge strategy. The importance is in managing vulnerabilities, protecting privacy, and enhancing the care provided to expectant mothers. The suggested approach offers a thorough resolution, enhancing the security of healthcare data and paving the way for improvements in safety systems throughout the healthcare spectrum. According to Hutchings et al. [16], to encourage the public to utilize health data for research, health organizations, and data custodians must clearly explain data security regulations to the public,

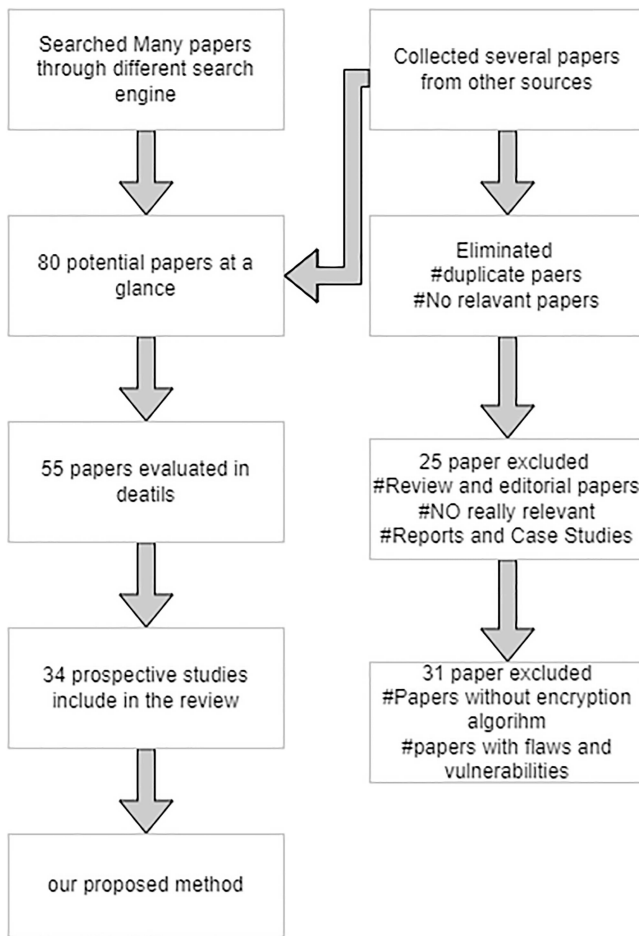


Figure 10.1 PRISMA schema for this study.

including when and by whom their data may be used. Similarly, Prez- Luet et al. [17], pregnant women want tailored health information that is clear, safe, and welcoming to maximize the comprehension of their pregnancy, adhere to advice, and achieve the best possible health outcomes. Strand et al. [18] concludes that although the information we utilize about pregnancies is sensitive, we firmly think that the advantages of making it more freely available would exceed the dangers. According to Kamoun and his colleague [19], SCM ideas can aid healthcare professionals in evaluating the risks and vulnerabilities related to the upkeep and dissemination of protected health information. Hackett et al. [20] found that deploying new technology to record healthcare user data during pregnancy and delivery positively and negatively impacts privacy and confidentiality. According to Scholas et al. [21], patient privacy and security are the most significant barriers to using meaningful

health data in electronic healthcare sectors. Shrivastava et al. [22] offer specific policy considerations, To increase the interoperability of health information while maintaining the security and privacy of patient data. Dan et al. [23] proposed an LDOS attack detection solution depend on several web activity characteristics and an enhanced Adaboost algorithm. Meng et al. [24] proposed a behavioral profiling-based trust-based intrusion detection approach (TBIDA) that was quicker than previous approaches in identifying rogue MSN nodes. According to Alloghani et al. [25], homomorphic encryption can maintain the CIA trinity while ensuring security and privacy in massive data and cloud computing. Catak et al. [26] recommend new clustering approaches that ensure privacy in conjunction with homomorphic encryption algorithms that can run on a conventional high-performance computing system, such as a cloud system. Rohila et al. [27] demonstrated that Homomorphic encryption is a more secure and safe option for creating a system that protects data from the server. It offers a way to perform calculations on the cipher text without disclosing anything about the plaintext to the server. According to Sustisna et al. [28], homomorphic encryption benefits cloud analytics and secure network communications. Cheng et al. [29] developed a patient privacy model using federated learning verification, combining encryption, blockchain, and federated learning for secure medical records. Vizitsu et al. [30] suggest Homomorphic encryption to minimize computational burden and safeguard data security, but the decryption of the key is risky. Data is uploaded to external servers to ensure security, but the plan needs to be more encrypted during transfer. Hussain et al. [31] has shown that the two most prevalent forms of assaults responsible for healthcare data breaches are unauthorized internal disclosures and hacking/IT incidents. According to research by Gao et al. [32], risks of service/operation interruption and risks of a data breach are the two cybersecurity concerns that are most frequently mentioned. Varshavsky et al. [33] found that pregnancy could lead to higher health risks for women and increase their susceptibility to environmental pollutants. At the same time, differences in research design and exposure measurement hindered the capacity to compare studies. Nellums et al. [34] sheds light on the experiences of pregnant women in the UK, focusing on the challenges posed by the country's increasingly stringent health regulations, which encompass payment obligations and data sharing. According to Cannon et al.'s research [35], women obtain online material that does not adhere to the most recent evidence-based recommendations.

According to Comfort et al. [36], free home pregnancy tests can enhance prenatal care by drawing more clients at risk of becoming pregnant to community-based health services, allowing them to confirm their pregnancy and get antenatal counseling. According to Khaki et al. [37], health professionals should enlighten women about prenatal care to alter their risk and persuade them to seek pertinent medical services. Hackett et al. [38] showed how using modern technologies to collect healthcare user data during pregnancy and delivery may have positive and negative effects on people's views of their privacy and confidentiality. Blatt et al [39] describe a homomorphic encryption-based privacy-preserving system that can

perform accurate GWAS analysis for a dataset of 25,000 individuals while keeping all personal information encrypted and requiring no user input. Wood et al. [40] describe that rapid and precise medical classification using private-key fully homomorphic encryption is possible. Scheibner et al. [41] show that multiparty homomorphic encryption meets the EU General Data Protection Regulation legal criteria for medical data exchange, ensuring global data protection standards.

10.2.1 Systematic Review

Here, we compare all papers from the literature review where we can easily show the pros and cons of these papers and where they can improve in the future.

10.3 Methods and Materials

In the previous section, we have seen that different researchers used different methods, frameworks, and models to improve the security of medical cyber-physical systems. However, it is crucial to recognize that standard algorithms run the danger of being intrusive for sensitive data, such as pregnancy data. As a result, this study aims to examine the effectiveness of homomorphic encryption as a solid strategy for creating a highly secure and dependable model for the medical cyber-physical system, focusing on its use in data about pregnancy. Figure 10.2 illustrates a simple approach used in this work. Where we have the initial pregnancy data, we will employ the homomorphic encryption strategy, then store that data and allow users to access plain text only after conducting decryption. Further elaboration on our proposed methodology will follow below.

10.3.1 Homomorphic Encryption

A sophisticated cryptographic method called homomorphic encryption enables computations on encrypted data without decryption. In order to protect the privacy and confidentiality of sensitive information, it enables data to stay encrypted during various processes. Homomorphic encryption aims to improve data security and shield private information from unwanted access or disclosure. Security of sensitive data, such as personal or medical information, benefits significantly from homomorphic encryption. It overcomes the intrinsic flaw in conventional encryption techniques, where data must first be decrypted to be processed or analyzed. As a result of the data being exposed in its unencrypted form during the decryption process, there is a possible vulnerability that leaves it open to intrusion or assault. A homomorphism is a map that preserves the structure of two identical algebraic structures, such as two groups, two rings, or two vector spaces. In other words, a map $f: N \rightarrow M$, $f: N \rightarrow M$ between two sets N , M outfitted with the same structure such that

Study id	Method	Research Objectives	Key Findings	Limitations	Conclusions
1. [16]	Systematic review	Analyze public attitudes toward linked health data research	Public support linked health data research lacks consensus on consent	Review studies vary across countries, limiting generalizability	The review emphasizes public engagement, education, and policy development for linked health data
2.[17]	Searched database to assess quality and bias	Healthcare consumers' attitudes towards consent and use of data for research	Increase awareness of data sharing and protection in patient populations	Search is limited to the English language publications, excluding relevant literature	Provide individuals with information and the choice of health data use
3.[18]	Diagrams guide statistical models	Determine the causality of relations between environmental exposures and birth outcomes	Ambient temperature increases the risks of preterm birth and stillbirth	The possibility of residual confounding due to imperfect measurement or unmeasured confounders	Further research is needed to determine causal relationships between environmental exposures and birth outcomes
4.[19]	The Swiss Chess Model's unstructured approaches	Highlight the importance of organizational policies and practices in preventing data breaches in healthcare	Many healthcare organizations are unprepared to prevent, cope with, or respond to a data breach	The paper does not provide specific solutions for preventing data breaches	Implementing a data safety culture and solid organizational policies protect healthcare

5.[20]	Qualitative research method	Explore frontline health workers' data security and Privacy perspectives in Tanzania	New technologies impact privacy and confidentiality perceptions during pregnancy and childbirth	The study was conducted in a specific context and may not be generalizable to other settings	Community-based engagement crucial for Health intervention development, incorporating beliefs and gender dynamics
6.[21]	Cloud computing and electronic communication, including HIPAA compliance	Examines healthcare data security and HIPAA compliance for patient protection	HIPAA compliance is an effective method for securing patient data in the healthcare industry	It does not explore other methods for healthcare data security technology in depth	Healthcare data security is crucial and HIPAA compliance is an essential method for achieving it
7.[21]	used a quasi-experimental research design	Examine security measures, privacy regulations, and communication standards are impacting patient health information	Access control measures on workstations reduce technical interoperability problems	Inability to investigate specific privacy regulations and communication standards linked to interoperability problems	Compatibility checks and usage guidelines are necessary for adopting new communication standards to avoid interoperability problems
8.[22]	MF-Adaboost	detect low-rate denial of service (LDOS) attacks using multiple features and an	The proposed method T shows improved performance in	It does not address the adaptability of the detection threshold to	The proposed method has a better anti-interference performance and

(Continued)

Study id	Method	Research Objectives	Key Findings	Limitations	Conclusions
		improved Adaboost algorithm	detecting LDoS attacks compared to e	changes in the environment	feasibility in detecting LDoS attacks
9.[22]	CLS scheme based on NTRU lattice	Proposal of NTRU lattice CLS scheme for efficient, secure MCPS, ensuring patient information integrity	NTRU lattice is both efficient and secure for use in medical cyber-physical systems	Design flaws and high/impractical computation	Secures patient information integrity in MCPS
10.[23]	PRISMA framework	Explore the status and progress of homomorphic encryption technologies	Homomorphic encryption is a significant part of security development	Lack of engagement in full text screening and data extraction	Homomorphic encryption is crucial for security development, requiring quantum computing for applications
11.[24]	Partially homomorphic encryption algorithm	Implement privacy-preserving clustering methods	The successful implementation of privacy-preserving clustering methods	Protecting privacy may have limitations in terms of scalability and efficiency	Data privacy is crucial; cloud service providers' mistrust is addressed

12. [25]	Homomorphic encryption	Implement k-nearest neighbor algorithm while preserving user location privacy using homomorphic encryption Proposal of a systolic	Size of 32 bits is appropriate to make the system work efficiently and securely	The system may not be practically possible for an arbitrary number of operations on encrypted data	Homomorphic encryption secures plaintext calculations without server knowledge, making it safer
13. [26]	Systolic array design	Array design for polynomial multiplication in homomorphic encryption	Optimized designs can be implemented in the PYNQ-Z1 board	Some designs cannot be implemented in PYNQ-Z1 board	Array design can be used for secure network communications and cloud analytic
14. [27]	Privacy-enhanced Data Fusion Strategy	A PDFS to ensure data security and privacy of COVID-19 applications in IoMT	PDFS enhances COVID-19 task classification accuracy, reliability, and privacy	PDFS has not been implemented in a real-world scenario	PDFS improves data security and privacy in COVID-19 IoMT applications
15. [28]	Dual signature ECDSA method	Improve security and privacy in IoMT communication through edge computing	The proposed method ensures data source anonymity, integrity, and authentication without computational complexity	The proposed method may face congestion in case of a high number of IoMT devices	The proposed method is a novel solution to enhance security and preserve data privacy in IoMT scenarios

(Continued)

Study id	Method	Research Objectives	Key Findings	Limitations	Conclusions
16. [42]	Blockchain, homomorphic encryption, and federated learning	Protect patient information privacy while promoting the development of medical technology Research explores	Achieves open patient records and collaborative diagnosis without compromising privacy	The experiment only used breast cancer patients data, and further validation is needed	Model safeguards patient privacy enables data sharing, and promotes precision medicine development
17. [43]	Deep learning-based ciphertext data analysis framework	Data privacy, enabling neural network computations over encrypted data	Method secures data privacy while enabling neural network computations	The experiments were not aimed at achieving state-of-the-art results for the proposed problems	Research suggests a secure medical data processing method
18. [29]	Data analysis method	Investigate healthcare data breaches and their causes and consequences	Healthcare industry vulnerable to 536 data breaches in 2018	Only analyzed data breaches reported	Healthcare data breaches demand enhanced security measures
19. [30]	Content analysis	Analyze the linguistic characteristics of cybersecurity risk disclosures in financial reports	Companies tend to use more litigious language in their cybersecurity risk disclosures	It only focuses on linguistic characteristics	The study recommends improving cybersecurity risk disclosure the clarity for investors and stakeholder information

20. [31]	Content analysis	The text discusses exposure quartiles, pregnancy impacts, gestational diabetes, and arsenic levels	Pregnancy increases lead exposure, causing hypertensive disorders	GDM assessment in the second trimester may limit early detection	Pregnancy exposome impacts maternal health; research needed
21. [32]	Scoping review method	Explore UK maternity care access experiences of undocumented migrants	Undocumented migrants face barriers to maternity care, affecting health	The study focuses on specific UK undocumented migrant women	Facilitate maternity care for undocumented migrant women to improve health outcomes
22. [33]	Systematic online search	Review pregnancy nutrition, physical activity, sleep websites, and evidence-based guidelines	women are accessing information via the internet is not in accordance with current evidence-based guidelines	It only focuses on the Australian government and leading industry websites	Government and industry websites must update information with evidence-based guidelines
23. [34]	Randomized controlled trial method	Evaluate the impact of free home pregnancy tests on women seeking antenatal care counseling	Free home pregnancy tests enhance remote antenatal counseling	Conducted in a specific region and may not be generalizable to other settings	Community-based pregnancy tests improve care-seeking in sub-Saharan Africa
24. [35]	Cross-sectional study	Identify the factors associated with	Wealth index birthplace,	Study limited to recent births and	Improve antenatal care access and encourage

(Continued)

Study id	Method	Research Objectives	Key Findings	Limitations	Conclusions
		postnatal care utilization among Malawian women	antenatal care visits significantly impact postnatal care utilization	excluded outside health facilities	women to give birth in health facilities
25.[36]	Study is qualitative	Explore frontline health workers' data security and privacy perspectives in Tanzania	Health enhances community health, but raises privacy and confidentiality concerns. HE framework	New technologies impact privacy and confidentiality in pregnancy and childbirth	The study suggests that community-based engagement is crucial for Health intervention integration
26.[37]	Homomorphic encryption (HE)	Accurate GWAS analysis on 25,000+ individuals securely	Accurately analyzes GWAS datasets, evaluating 100,000 individuals and SNPs in 5.6 hours	HE solution is faster than MPC solutions by over one order of magnitude	The conclusion is that the HE can be applied to other domains where large-scale statistical analyses of encrypted data are needed
27.[38]	Private-key fully homomorphic encryption	Provide a method for private classification of medical data without compromising patients' privacy	Private-key fully homomorphic encryption can provide fast and accurate results for privacy-preserving medical classification	The size of the input grows exponentially with each multiplication performed	The proposed protocol effectively classifies breast cancer data for privacy

28. [39]	Homomorphic encryption	Explore privacy-enhancing technologies for medical data sharing	Homomorphic encryption and secure multiparty computation ensure privacy in medical data sharing	Homomorphic encryption complex, may not be suitable for low-power devices	Update regulatory instruments and address ethical concerns in privacy-enhancing technologies
29. [40]	Systolic array design	Proposal of a systolic array design for polynomial multiplication in homomorphic encryption	The paper reveals a systolic array design accelerates polynomial multiplication in the PYNQ-Z1 board	The clock speed decreases for bigger designs and some designs cannot be implemented in the PYNQ-Z1 board	Proposed systolic array design for polynomial multiplication in homomorphic encryption optimized for hardware implementation

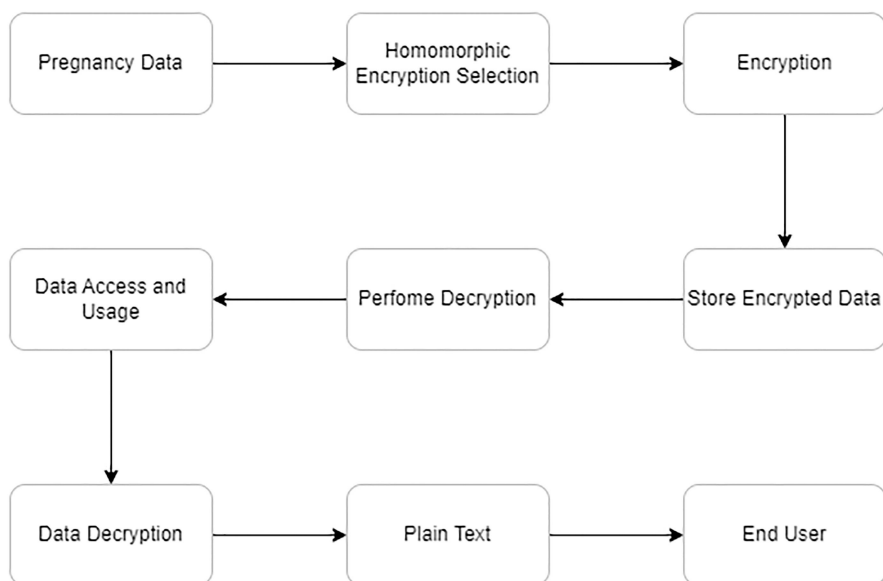


Figure 10.2 Block diagram outlining the overview process.

$$F(N \times M) = F(N)(M) \quad (10.1)$$

It is possible to operate with encrypted data using homomorphic encryption without first needing to decrypt it. Homomorphic encryption algorithms employ both symmetric-key and public-key encryption methods. Three main kinds of homomorphic encryption exist: Somewhat homomorphic, substantially homomorphic, and fully holomorphic. Generally speaking, homomorphic encryption comes in three different flavors.

Partially Homomorphic Encryption: With partially homomorphic encryption techniques, performing a single operation, such as addition or multiplication, is possible while preserving the encryption. The Paillier cryptosystem is one example of a partially homomorphic encryption method allowing secure addition operations on encrypted data. Fully Homomorphic Encryption (FHE): FHE techniques allow calculations while preserving the encryption for addition and multiplication operations. This implies that any computations, including arbitrary ones, can be made on encrypted data without decryption. However, compared to partly homomorphic encryption techniques, FHE systems often require greater processing power. A well-known instance of completely homomorphic encryption is the Gentry system.

Somewhat Homomorphic Encryption (SHE): Between partially homomorphic and completely homomorphic encryption, somewhat homomorphic encryption techniques achieve an equilibrium. They preserve encryption while allowing for a

finite amount of calculations on encrypted data. Compared to partially homomorphic methods, this enables more complicated computations while requiring less processing effort than completely homomorphic encryption. It is commonly known as the Brakerski-Gentry-Vaikuntanathan (BGV) scheme.

To execute certain computations on encrypted data without the requirement for decryption, partially homomorphic encryption is used. It permits operations on encrypted values like addition and multiplication while maintaining the privacy of the underlying data. This feature is helpful when it is necessary to make computations on delicate information, like pregnancy data, while keeping it safe from unwanted access. Encryption that is only partially homomorphic finds a compromise between security and computing effectiveness, providing a workable option for applications that only need a small amount of homomorphism. Several types of Schemes are available for homomorphic encryptions. Table 10.1 shows the differences between them.

Pallier encryption algorithm works better. We choose Paillier encryption over these. Because of its additive homomorphism and semantic security characteristics, Paillier encryption is frequently used. It is appropriate for applications that need calculations, such as data aggregation or secure voting systems, because it enables safe addition and scalar multiplication operations on encrypted information. Furthermore, Paillier encryption offers defense against specific plaintext and ciphertext assaults, guaranteeing the security of sensitive data. It is noninteractive-ness and ease of use are other factors in its appeal for secure data transport.

10.3.2 Homomorphic Encryption in Data Security

The security and privacy of sensitive information are guaranteed by homomorphic encryption, a cutting-edge technique that enables calculations on encrypted data without decryption. It offers partial or complete homomorphism, allowing specific operations or arbitrary computations on encrypted data. It brings several advantages to data security, such as protecting sensitive data from unauthorized access, data breaches, and insider attacks, facilitating secure data sharing and collaboration while preserving privacy, and enabling privacy-preserving data analysis and computation. However, it is essential to consider the computational overhead and the performance implications of homomorphic encryption, particularly with fully homomorphic encryption. Homomorphic encryption emerges as a potent technology, guaranteeing secure data processing and analysis while safeguarding data privacy. This breakthrough paves the way for secure data sharing, collaboration, and advanced analytics.

10.3.3 Homomorphic Encryption in Data Transmission

Homomorphic encryption is an attractive option for securing sensitive information during data transmission, as it allows for computations on encrypted data without decryption. By applying homomorphic encryption to data before transmission, the data remains encrypted and unintelligible to any unauthorized party intercepting

Table 10.1 Comparison of Homomorphic Encryption Algorithms

<i>Homomorphic Encryption Algorithm</i>	<i>Level of Homomorphism</i>	<i>Security Level</i>	<i>Performance (Operations/s)</i>	<i>Data Transmission Speed (Mbps)</i>	<i>Ease of Implementation (1–10)</i>
Paillier	Partially Homomorphic	High	5,000	100	9
FHE	Fully Homomorphic	Very High	10	1	3
SHE	Somewhat Homomorphic	High	2,000	50	8

the communication, ensuring the confidentiality of the transmitted data. During data transmission, homomorphic encryption permits some calculations on the encrypted data without decoding it, such as addition or multiplication operations. Organizations can protect sensitive data from unauthorized access and maintain its confidentiality throughout communication by utilizing homomorphic encryption for data transmission. However, it is essential to consider the computational overhead associated with homomorphic encryption, as it can impact the transmission speed and efficiency. Overall, using homomorphic encryption for data transmission allows for secure communication while preserving the confidentiality of transmitted information.

10.4 Our Proposed Model

- **Collection of Pregnancy Data Using Smart IoT Devices:** Use wearables, smart scales, blood pressure monitors, fetal Dopplers, intelligent pillows, and smart thermometers to collect all the data needed about pregnancy. These tools collect vital information for a pregnant woman's health and well-being, including her activity levels, sleep habits, heart rate, weight, blood pressure, and fetal heart rate.
- **Homomorphic Encryption of Data:** To preserve data privacy, use a robust homomorphic encryption technique. The encryption method of choice should provide calculations on the encrypted data without decryption using both additive and multiplicative operations. Concentrate on enhancing the homomorphic encryption algorithm's performance to reduce computational costs and preserve the integrity and secrecy of data.
- **Secure Transmission and Storage:** The Secure Delivery and Storage model provides secure delivery of encrypted pregnant health data using robust cryptographic protocols like HTTPS or SSL. A cloud storage system with strict security controls is utilized for safe storage, and end-to-end encryption is employed to protect data during transmission over public networks. Key management is put into place to guarantee data confidentiality and integrity during transmission and storage, access controls, strong data encryption, and safe encryption.
- **Data Analysis and Treatment:** Authorized healthcare practitioners can safely access encrypted data for analysis and treatment. To decode the data while maintaining data privacy, sophisticated decryption techniques are used in restricted situations. Doctors can analyze the data and offer individualized care thanks to the thorough reports created. Strict access controls, authentication procedures, and audit trails are implemented to stop illegal access and guarantee data privacy.
- **Performance Optimization:** To increase the efficiency of the homomorphic encryption method, the suggested model integrates optimization strategies such

as hardware acceleration and algorithmic optimizations. With no compromise to data security, this enables real-time data processing and analysis.

- **Key Management and Security:** The necessary management procedures used by the model are robust and include systems for safe key creation, distribution, storage, and revocation. Additionally, it focuses on identifying and countering future encryption key-targeting attacks through ongoing surveillance and proactive security measures.
- **Usability and User Experience:** By creating an intuitive interface and user-friendly functions, the model prioritizes usability and user experience. To iteratively enhance the system's usability and reduce the cognitive strain on users, feedback from healthcare experts and users is gathered.
- **Interoperability and Integration:** The suggested paradigm adopts established protocols and data formats for smooth interaction with intelligent IoT devices, and healthcare systems to overcome interoperability problems. Thorough testing and validation ensure that components work together and share data effectively.
- **Regulatory Compliance:** To guarantee compliance with pertinent laws like HIPAA or GDPR, architecture includes methods for data consent management, data retention policies, and safe data erasure. Strictly adhering to regulatory regulations keeps sensitive patient information private and confidential.
- **Security Auditing and Monitoring:** A robust security auditing and monitoring system is implemented to identify possible security breaches or abnormalities and take appropriate action. Data integrity is maintained, vulnerabilities are identified, and risks are reduced using routine audits, log analysis, and proactive monitoring techniques.

The security of prenatal health data during transmission may be significantly improved using the suggested advanced paradigm. The model includes robust key

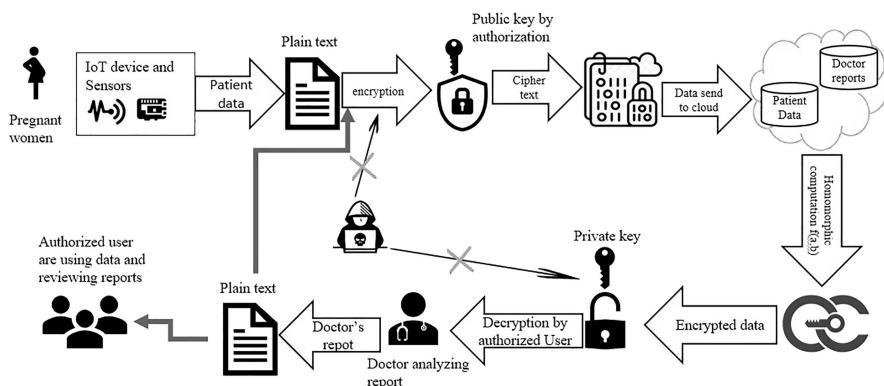


Figure 10.3 Proposed methodology for enhancing security of pregnancy health data transmission.

management, efficient performance, safe transmission and storage, interoperability, strong encryption, user-friendly interfaces, regulatory compliance, and ongoing security monitoring to ensure secrecy (Figure 10.3).

10.5 Activity Diagram

Doctors and patients must request information to register and assign doctors shown in Figure 10.4 (1, 1.1). This process also includes validation and homomorphic-based assignment. Once they have checked the info, the hospital folks connect a patient with a doctor. All health-related data is continuously gathered and securely stored within our system. Any deviations from the norm are promptly reported to the relevant parties. The process for managing this task, referred to as “activity 2,” is detailed in the accompanying figure. Each data upload and access instance is meticulously logged in our ledger as a transaction. To preserve all monitoring data, we employ cloud storage solutions.

Medical professionals are granted access to a patient’s monitoring information, with the workflow outlined in “activity 3.13.3”: When a doctor seeks access to a patient’s data, they initiate a request within our system. To confirm the doctor’s identity, the patient must provide their authorization key (activity 3.1). Upon

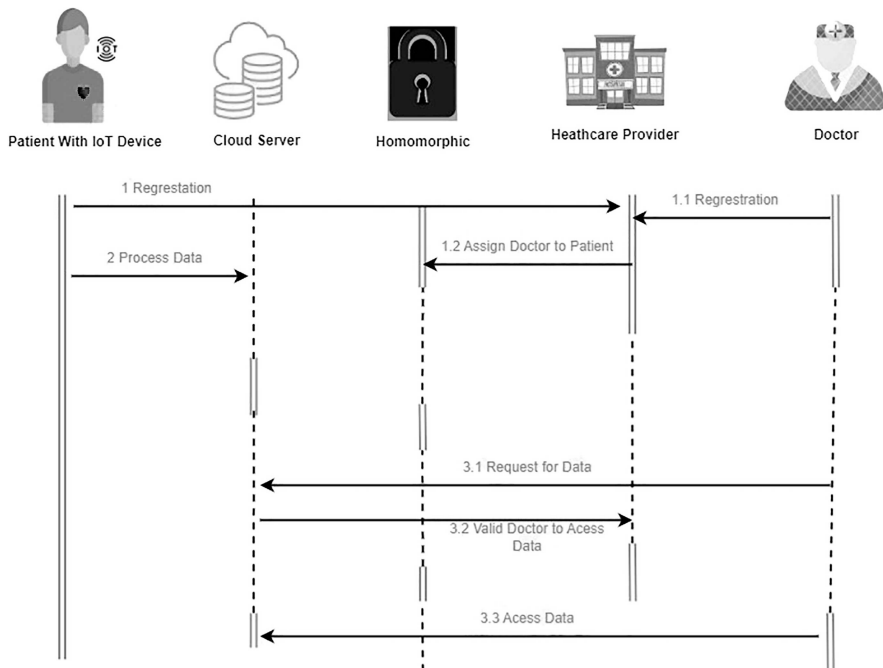


Figure 10.4 Activity diagram of proposed method.

receiving the doctor's request, a smart contract is initiated to validate the doctor's legitimacy before permitting access to the patient's data (activity 3.2). Once the doctor's credentials are verified within our system (activity 3.3), they access the patient's data stored in the ledger. This version maintains a formal tone appropriate for a paper while providing clear and concise explanations of the processes involved.

10.6 Conclusion

The sophisticated model presented for applying homomorphic encryption to secure pregnant health data during transmission provides a thorough and reliable method for protecting sensitive information. It emphasizes performance optimization, key management, usability, interoperability, and regulatory compliance to handle crucial data security areas. The concept may increase security and privacy controls by including multi-factor authentication, data masking, secure hardware modules, and privacy-preserving analytics. Integrating blockchain technology may improve accountability and transparency, and secure firmware and software upgrades protect the system's integrity. The suggested methodology strongly emphasizes ongoing security testing, auditing, and monitoring to find possible threats and vulnerabilities and take appropriate action. The approach offers a solid base for protecting sensitive healthcare data and establishing confidence in data transmission procedures by abiding by legal standards, enforcing rigorous access restrictions, and considering user input

References

1. R. Hamza, K. Zettsu, Investigation on privacy-preserving techniques for personal data, in: *Proceedings of the 2021 Workshop on Intelligent Cross-Data Analysis and Retrieval*, 2021, pp. 62–66.
2. N. M. Nayan, A. Islam, M. U. Islam, E. Ahmed, M. M. Hossain, M. Z. Alam, Smote oversampling and near miss undersampling based diabetes diagnosis from imbalanced dataset with XAI visualization, in: *2023 IEEE Symposium on Computers and Communications (ISCC)*, IEEE, 2023, pp. 1–6.
3. A. K. Singh, H. Zhou, S. Berretti, Guest editorial: Medical data security solution for healthcare industries, *IEEE Transactions on Industrial Informatics* 18 (8) (2022) 5558–5560.
4. F. Akter, M. A. Kashem, M. M. Islam, M. A. Chowdhury, M. Rokunojjaman, J. Uddin, Cyber-physical system (CPS) based heart disease's prediction model for community clinic using machine learning classifiers, *Journal of Hunan University Natural Sciences* 48 (12) (2021).
5. M. S. Rathore, M. Poongodi, P. Saurabh, U. K. Lilhore, S. Bourouis, W. Alhakami, J. Osamor, M. Hamdi, A novel trust-based security and privacy model for internet of vehicles using encryption and steganography, *Computers and Electrical Engineering* 102 (2022) 108205.

6. G. P. Reddy, A. Narayana, P. K. Keerthan, B. Vineetha, P. Honnavalli. Multiple hashing using SHA-256 and MD5 lecture notes in electrical engineering, *Advances in Computing and Network Communications* (2021) 643–655. 10.1007/978-981-33-6977-1_47
7. M. N. Alenezi, H. Alabdulrazzaq, N. Q. Mohammad, Symmetric encryption algorithms: Review and evaluation study, *International Journal of Communication Networks and Information Security* 12 (2) (2020) 256–272.
8. P. Khatriwada, S. Joshi, K. M. Mohan, K. Chouhan, D. Gangodkar, Z. Z. Khan, Design a wireless network data security system for medical records using cryptography, in: 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, 2022, pp. 207–211.
9. M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A.-H. A. Hashim, S. Habib, M. Islam, S. Alyahya, M. M. Ahmed, S. Kamil, et al., Lightweight encryption technique to enhance medical image security on internet of medical things applications, *IEEE Access* 9 (2021) 47731–47742.
10. W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, F. Qian, Secure control of multiagent systems against malicious attacks: A brief survey, *IEEE Transactions on Industrial Informatics* 18 (6) (2021) 3595–3608.
11. A. Longras, H. Oliveira, S. Paiva, Security vulnerabilities on implantable medical devices, in: 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, 2020, pp. 1–4.
12. J. Li, X. Liang, C. Dai, S. Xiang, Reversible data hiding algorithm in fully homomorphic encrypted domain, *Entropy* 21 (7) (2019) 625.
13. D. Franco, L. Oneto, N. Navarin, D. Anguita, Toward learning trustworthily from data combining privacy, fairness, and explainability: An application to face recognition, *Entropy* 23 (8) (2021) 1047.
14. X. Wang, L. Bai, Q. Yang, L. Wang, F. Jiang, A dual privacy-preservation scheme for cloud-based ehealth systems, *Journal of Information Security and Applications* 47 (2019) 132–138.
15. I. Sudha, R. Nedunchelian, A secure data protection technique for healthcare data in the cloud using homomorphic encryption and Jaya–Whale optimization algorithm, *International Journal of Modeling and Simulation, and Scientific Computing* 10 (06) (2019) 1950040.
16. E. Hutchings, M. Loomes, P. Butow, F. M. Boyle, A systematic literature review of attitudes towards secondary use and sharing of health administrative and clinical trial data: A focus on consent, *Systematic Reviews* 10 (2021) 1–44.
17. J. E. Pe´rez-Lu, A. M. Bayer, R. Iguin´iz-Romero, Information= equity? how increased access to information can enhance equity and improve health outcomes for pregnant women in Peru, *Journal of Public Health* 40 (suppl 2) (2018) ii64–ii73.
18. L. B. Strand, A. G. Barnett, S. Tong, Strand et al. respond to environmental exposures and preterm birth, *American Journal of Epidemiology* 175 (2) (2012) 113–113.
19. F. Kamoun, M. Nicho, Human and organizational factors of healthcare data breaches: The Swiss cheese model of data breach causation and prevention, *International Journal of Healthcare Information Systems and Informatics (IJHISI)* 9 (1) (2014) 42–60.
20. K. M. Hackett, M. Kazemi, D. W. Sellen Keeping secrets in the cloud: Mobile phones, data security and privacy within the context of pregnancy and childbirth in Tanzania. *Social Science & Medicine* 211 (2018) 190–197. 10.1016/j.socscimed.2018.06.014.

21. S. Mbonihankuye, A. Nkuzimana, A. Ndagijimana (2019). Healthcare Data Security Technology: HIPAA Compliance. *Wireless Communications and Mobile Computing*, 2019, 1–7. 10.1155/2019/1927495.
22. U. Shrivastava, J. Song, Han B. T., D. Dietzman Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation. *International Journal of Medical Informatics* 148 (2021) 104401. 10.1016/j.ijmedinf.2021.104401.
23. D. Tang, L. Tang, R. Dai, J. Chen, X. Li, J. J. Rodrigues, Mf-AdaBoost: LDOS attack detection based on multi-features and improved AdaBoost, *Future Generation Computer Systems* 106 (2020) 347–359.
24. Z. Xu, D. He, P. Vijayakumar, K.-K. R. Choo, L. Li, Efficient NTRU lattice-based certificateless signature scheme for medical cyber-physical systems, *Journal of Medical Systems* 44 (2020) 1–8.
25. M. Alloghani, M. M. Alani, D. Al-Jumeily, T. Baker, J. Mustafina, A. Hussain, A. J. Aljaaf, A systematic review on the status and progress of homomorphic encryption technologies, *Journal of Information Security and Applications* 48 (2019) 102362.
26. F. O. Catak, I. Aydin, O. Elezaj, S. Yildirim-Yayilgan, Practical implementation of privacy preserving clustering methods using a partially homomorphic encryption algorithm, *Electronics*, 9 (2020) 229. 10.3390/electronics9020229.
27. A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, R. Ahmad Khan, Healthcare data breaches: Insights and implications. *Healthcare*, 8 (2020) 133. 10.3390/healthcare8020133.
28. L. Gao, T. G. Calderon, & F. Tang (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, 38, 100468. 10.1016/j.accinf.2020.100468.
29. S. Cannon, M. Lastella, L. Vincze, C. Vandelanotte, & M. Hayman (2020). A review of pregnancy information on nutrition, physical activity and sleep websites. *Women and Birth*, 33, 35–40. 10.1016/j.wombi.2018.12.007.
30. A. Comfort, Do home pregnancy tests bring women to community health workers for antenatal care counselling? A randomized controlled trial in Madagascar. *Health Policy and Planning*.
31. A. B. Comfort, R. C. Juras, S. E. K. Bradley, J. Ranjalahy Rasolofomanana, A. Noeliarivelo Ranjalahy, C. C. Harper (2019). Do home pregnancy tests bring women to community health workers for antenatal care counselling? A randomized controlled trial in Madagascar. *Health Policy and Planning*, 34, 566–573. 10.1093/heapol/czz080.
32. J. Khaki (2019). Factors associated with the utilization of postnatal care services among Malawian women. *Malawi Medical Journal*, 31, 2. 10.4314/mmj.v31i1.2.
33. K. M. Hackett, M. Kazemi, D. W. Sellen, Keeping secrets in the cloud: Mobile phones, data security and privacy within the context of pregnancy and childbirth in Tanzania, *Social Science & Medicine* 211 (2018) 190–197.
34. M. Blatt, A. Gusev, Y. Polyakov, S. Goldwasser, Secure large-scale genome-wide association studies using homomorphic encryption, *Proceedings of the National Academy of Sciences* 117 (21) (2020) 11608–11613.
35. A. Wood, V. Shpilrain, K. Najarian, D. Kahrobaei, Private naive Bayes classification of personal biomedical data: Application in cancer data analysis, *Computers in Biology and Medicine* 105 (2019) 144–150.

36. J. Scheibner, J. L. Raisaro, J. R. Troncoso-Pastoriza, M. Ienca, J. Fellay, E. Vayena, J.-P. Hubaux, Revolutionizing medical data sharing using advanced privacy-enhancing technologies: Technical, legal, and ethical synthesis, *Journal of Medical Internet Research* 23 (2) (2021) e25120.
37. N. Sutisna, G. Jonatan, I. Syafalni, R. Mulyawan, T. Adiono, Polynomial multiplication systolic array for homomorphic encryption in secure network communications, in: 2020 IEEE International Conference on Communication, Networks and Satellite (Comnetsat), IEEE, 2020, pp. 390–394.
38. V. Pathak, Lattices, homomorphic encryption, and CKKS, arXiv preprint arXiv:2205.03511.
39. S. Farah, Y. Javed, A. Shamim, T. Nawaz, An experimental study on performance evaluation of asymmetric encryption algorithms, in: Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science (EECS-12), 2012, pp. 121–124.
40. M. Blatt, A. Gusev, Y. Polyakov, S., Goldwasser, Secure large-scale genome-wide association studies using homomorphic encryption. *Proceedings of the National Academy of Sciences*, 117 (2020) 11608–11613. 10.1073/pnas.1918257117.
41. A. Wood, V. Shpilrain, K. Najarian, D. Kahrobaei, Private naive bayes classification of personal biomedical data: Application in cancer data analysis, *Computers in Biology and Medicine* 105 (2019) 144–150.
42. J. Scheibner, J. L. Raisaro, J. R. Troncoso-Pastoriza, M. Ienca, Fellay J., E. Vayena, J.-P., Hubaux, Revolutionizing medical data sharing using advanced privacy-enhancing technologies: Technical, legal, and ethical synthesis, *Journal of Medical Internet Research*, 23 (2021) e25120. 10.2196/25120.
43. J. Varshavsky, A. Smith, A. Wang, E. Hom, M. Izano, H. Huang, A. Padula, T. J. Woodruff, Heightened susceptibility: A review of how pregnancy and chemical exposures influence maternal health. *Reproductive Toxicology*, 92 (2020) 14–56. 10.1016/j.reprotox.2019.04.004.

Chapter 11

E-Health Data Acquisition System for Detection and Prevention of Cardiac Diseases Utilizing IoT

Adarsh Ravi Mishra¹ and Manoj Kumar Pandey^{2,3}

¹Department of CS & IT, Dr. C.V. Raman University, Bilaspur, Chhattisgarh, India

²Department of CS, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India

³Department of CSE, Chandigarh University, Mohali, Punjab, India

11.1 Introduction

11.1.1 Importance of IoT in Healthcare

The impending issues and social concerns of an aging population are being met thanks to recent developments in wireless networking, microelectronics, and wireless sensors. India's population is continually growing, and at the same time, the senior population is also growing. The use of cutting-edge technical solutions in hospitals has increased the expense of health maintenance as well. The monitoring of senior residents' health might be moved from hospital systems to those where they reside as an efficient solution to the issues mentioned above. With this approach, seniors may remain in their homes longer and have easier access to quality healthcare. Additionally, this might provide individuals greater independence while less expensively keeping an eye on their general health [1].

The objective is to create a health monitoring system that uses machine learning and the internet of things to monitor patient condition remotely. This device permits the transmission of both routine and emergency vital signs and may be used in both indoor and outdoor locations. The ECG signal is continuously monitored in order to estimate the patient's likelihood of having a heart attack. Using the proposed method the patient physiological data may be displayed, recorded, and sent using the system. Additionally, the suggested health surveillance system has web access, allowing healthcare practitioners to observe and retrieve patient information at any time from any location around the globe [2,3].

Instead of data stored on a local server and perhaps on other devices, the cloud methodology employs a network of cloud computers that are hosted on the web to save, maintain, and handle the data. The industries can compute resources that can be used as utilities with its help. Even services like electricity are possible. Biomedical sensors that are implanted in the patient convert variations in the physiological variables being tracked into electronic data that can be measured and collected. The sensor's data are sent via the GPRS network to a smart server.

The following four circumstances are ideal for the suggested e-health monitoring. Patients with physiologic regulatory systems that are unstable come first, such as those who have respiratory congestion as a result of a medication overdose or anesthesia. Patients in a suspected life-threatening scenario, such as a diagnostic that suggests a heart attack may occur, fall under the second category. Later group patients who have a high chance of getting an illness that might be fatal come under third other category.

Individuals in a critical physiological condition, such as those recuperating from a serious injury or an accident, are the fourth category of patients that need to be watched, and they need to be monitored [4–8]. Our technique is also intended for the elderly, who need ongoing observation for several occurrences of the aforementioned conditions [9]. This technology aims to speed up the detection of illnesses while simultaneously improving its efficiency and accuracy. It is also intended to provide the patient a constant feeling of safety by offering quick assistance in case of crises.

In our network infrastructure, the smart device plays a significant role in analyzing and transmitting data, functioning as a gateway and so lowering expenses. We designed this building with the possibility of its application in rural India, where healthcare facilities and hospitals are less well-equipped than those in metropolitan areas. This system with mobile sensors and smart gadgets can be used in various areas to determine a patient's diagnosis [10,11].

11.2 Literature Review

A health surveillance system, also recognized as a patient health monitoring device or wireless wearables for healthcare, involves wirelessly delivering patient data to distant locations while remotely observing a patient's vital signs using equipment.

Utilizing communication technology efficiently in the healthcare industry decreases the complexity of tracking multiple patients at the same time. It enables them to monitor patients without actually being by their bedsides, whether they are at home or at hospital [12,13]. The equipment utilizes several sensors to keep track of vital signs of patient including ECG, heart rate, respiration, non-invasive blood pressure, body temperature, oxygen saturation, and others. There have been many and steadily growing studies and research activities reported in the literature. Only a few of the most recent relevant works are included in this attempt due to time constraints. An indoor or outdoor real-time mobile healthcare system for aged healthcare management has been introduced in [14,15].

11.2.1 Wireless Health Supervision Apparatus

As mentioned previously utilizing communication technology in the healthcare industry reduces the complexity of tracking multiple patients at the same time. It enables them to monitor patients without actually being by their bedsides, whether they are in a hospital or at home [14,15].

11.2.2 Bio Signal Sensor

Biological signals are data registers that provide details about biological processes over a certain time period (i.e., a heartbeat). For doctors, scientists, and those involved in diagnosis, the analysis of these indications is extremely valuable. The system's two major parts are a smartphone and a bio signal detector. A smart server receives the data gathered by the bio signal sensor through a GPRS/UMTS network. The device enables remote monitoring of the elderly patients measure, whereabouts, and vital signs.

11.2.3 Electro Cardiogram (ECG)

The patient health may be constantly and in the moment monitored by the shirt using acceleration signals and electrocardiogram (ECG) measurements. In order to get the body signal, the shirt is mostly made of various sensors and conductive materials [16,17]. The measured body signals are sent using the GPRS network to the server PC. The wearable gadgets are tiny enough to fit inside a shirt and have low battery consumption. In this study, an adaptive threshold approach has also been presented in order to lessen the noise present in the ECG signal.

11.3 Methodology

This section contains the methodology used for the proposed work.

11.3.1 Context

By using a wireless sensors network, patient's medical values are tracked and transmitted to the remote site through GPRS interface. Microcontroller monitors data received at the far end. The GSM module is set up to propel an SMS to the doctor's cell device and to modify the data on the website if the variables are unusual. The system used in this chapter is designed for patients like these who aren't in a life-threatening situation but nevertheless need to be monitored regularly. The device will generate an alert message and transmit data to the concerned doctor when the emergency condition happens. It checks patients remotely from their homes and is quick and inexpensive. Figure 11.1 shows the system block diagram for the proposed work.

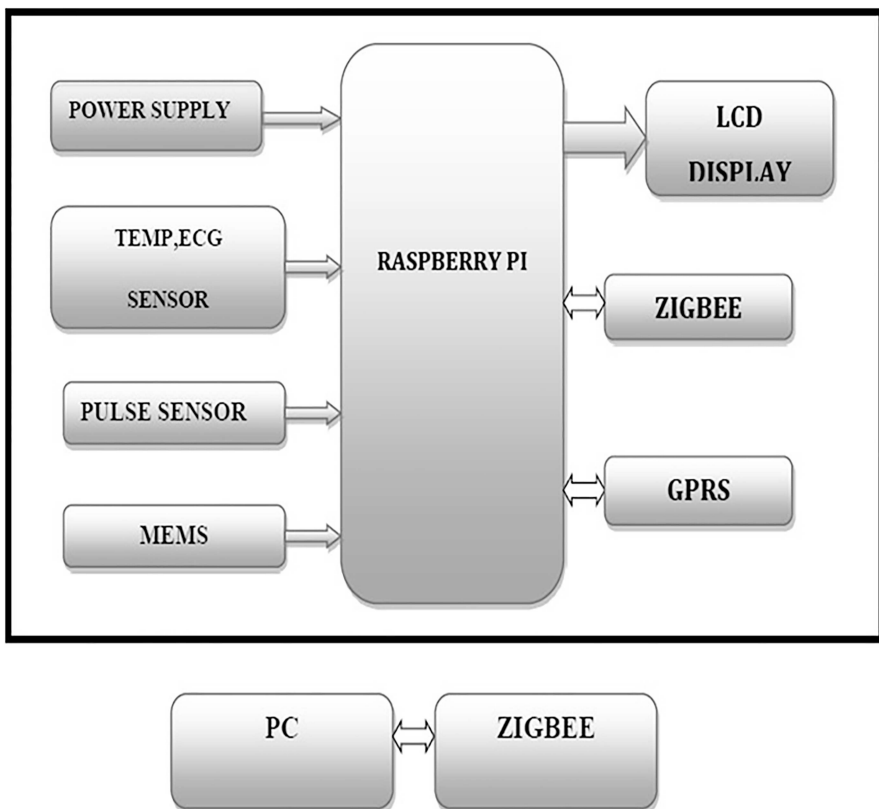


Figure 11.1 System block diagram.

Figure 11.2 depicts the planned job's work flow diagram. The instruments utilized for measuring blood oxygen saturation level, location or gesture of the person, and body temperatures are MAX30100, LM35, and MPU 6050,

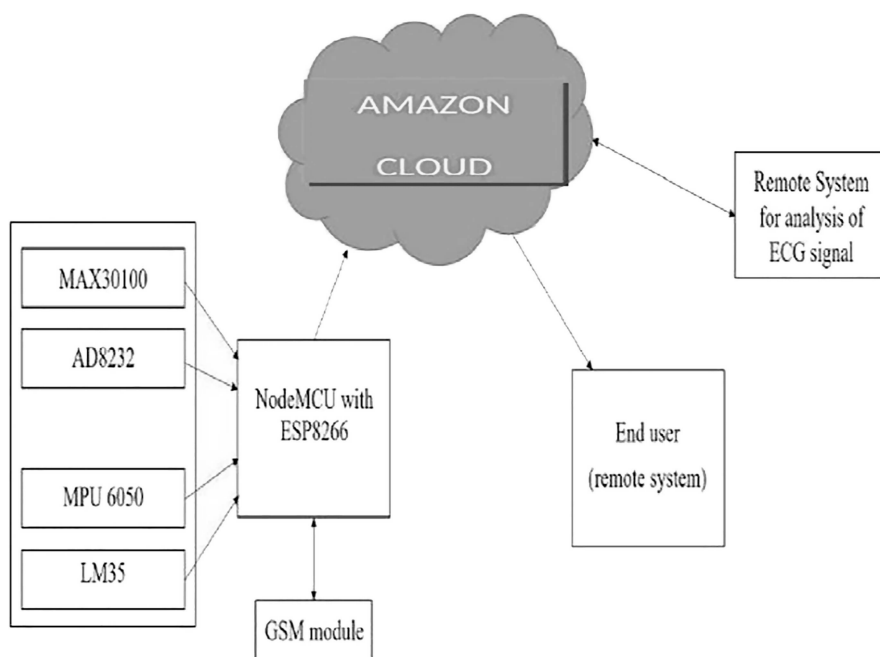


Figure 11.2 Flow diagram.

respectively. The capture of ECG signal for heart attack forecasting is done using the AD8232, which is an integrated signal conditioning block for electrocardiograms (ECGs). All of the sensors were chosen depending on how well they performed in detecting the various health markers.

The Node-MCU is linked to all of the sensors. There is an access point that the Node-MCU is linked to. The processor utilized in this study consists of two units: a Node-MCU microcontroller unit and an ESP8266 Wi-Fi unit for remote monitoring. The microcontroller sends the sensor data it has gathered to the ESP8266 for Wi-Fi cloud transmission. Amazon is the name of the cloud computing platform used for data processing and archiving. The customer can utilize an internet connection to access the Amazon. For parameter analysis and continual monitoring, the data stored in the cloud may be used. The data is communicated via the internet via the point of access. Packets of data are transmitted through a network. The data is received by the Amazon server and the ECG data retrieved from the Amazon server is used with machine learning algorithms to predict heart attacks [18].

11.3.2 Bio Monitoring Electrodes, Sensors and Components

Ionic action in living cells produces bio-potentials, which are electrical potentials inside the live organism. The ECG signal comes from the heart's action potentials.

These potentials appear on the surface of the body because of the conductivity of the human body. Ionic activity must be converted into electronic current using an electrode as the transducer. The skin's dry dielectric surface prevents ions from moving from the tissue to electrons in the electrode. Typically, a chloride gel or saline solution is used as a conducting link to connect the patient's skin to a silver/silver chloride detector.

The skin impedance, the impedance of the electrolyte gel, and the two layers at the electrode surface, as well as half-cell potentials caused by variable electrodes, electrolytes, and tissue energy, are all components of the electrical transducer. Micron's unique studs are the appropriate electrode component for the MRI, ER, XRAY, OR, Catheter Lab, or ICU because they combine radio delicate shading, MRI compatibility, and excellent signal quality. This robust, little stud is perfect for generating trustworthy ECG traces in a variety of applications.

11.4 Hardware Requirements

This section contains the details about all the hardware used for the research.

11.4.1 Raspberry Pi3 Model

The computing power of the Raspberry Pi3 is six times greater than that of earlier versions. This second-generation Raspberry Pi is equipped with an improved Broadcom BCM2837 CPU and a powerful quad-core ARM Cortex-A53 microprocessor that operates at 1.2 GHz. Additionally, the board has increased memory capacity to 1 Gigabyte.

11.4.2 Oscillating System

A piezoelectric diaphragm serves as the basic noise source of a piezoelectric audio constituent. A piezoelectric diaphragm (brass or stainless steel, etc.) is composed of a piezoelectric ceramic panel with electrodes on either side or a metal plate. A piezoelectric ceramic plate is attached to a metal plate using adhesives. When a piezoelectric diaphragm's electrodes are subjected to a D.C. voltage, the piezoelectricity causes structural deformation. A piezoelectric element with an incorrect shape will deform along a radial direction.

11.4.3 Pulse Sensor

Heartbeat sensors are another name for pulse sensors. A digital output of the heartbeat is created when a finger is inserted into this heartbeat sensor. While the heart sensor is in use, the uppermost LED flashes in rhythm with each heartbeat. Simply attaching this digital output to a microcontroller will allow you to calculate

the beats per minute (BPM) rate. It works on the principle that each pulse modifies the amount of light. Features include LED heart beat indicator, instant digital signal readout for microcontroller connection, small size, and working voltage of +5 V DC. The sensor is made up of a light detector and a very bright red LED. To pass through the fingertip and be recognized at the other end, the LED must be exceedingly bright. Less light was able to reach the sensors now that the finger is slightly more opaque when the heart pumps blood via the blood arteries. The detector signal changes with each heartbeat. This variation produces an electrical pulse. This signal is increased and activated by an amplifier that generates a +5 V logic-level signal. A top-mounted LED blinks in rhythm with each heartbeat as another indicator for the output signal.

11.4.4 Micro Electro Mechanical System (MEMs)

In order to construct Micro-Electro-Mechanical Systems (MEMS), the micro-fabrication technique is utilized to integrate mechanical components, detectors, controls, and technologies on a single silicon substrate. The technology is created using integrated circuit (IC) which processes sequences of CMOS, Bipolar, or BICMOS procedures, whereas the micromechanical elements are created using suitable micromachining processes that selectively inscribe away portions of the silicon wafer or create new hierarchical arrangements to create the mechanical and electromechanical equipment.

11.4.5 ZIGBEE Technology

A new wireless protocol called ZIGBEE is based on the IEEE 802.15.4 personal area networks standard. It is primarily intended to replace the current non-standard technologies and be used in a wide range of automation approach.

It now operates at a maximum data rate of 250Kbps in the 2.4 GHz ISM bands worldwide at 20Kbps in the 868 MHz band in Europe, and 40Kbps in the 914 MHz band in the USA. The ZIGBEE specification was produced by combining the home RF Lite and 802.15.4 specifications. The protocol uses the same 2.4 GHz (ISM) radio frequency as Bluetooth, the 802.11b technology, microwaves, and a few other devices. Per network, it can link up to 255 devices [19,20].

11.4.6 Alternative Main Processing Devices

Although there were many other options, the Raspberry Pi3 model is selected as the system's primary processor. Arduino, Intel Edison, different tablet and computer (laptop) models, and even cell phones are additional options that can be used. All of these units have the processing power required to complete these jobs, but they were missing several crucial capabilities for this project.

11.4.6.1 *Arduino*

Arduino is a microcontroller rather than a computer. The Raspberry Pi, for example, differs in that it features a processing unit for graphics and sound as well as the capacity to attach peripherals through USB, for example. An Arduino device does not have any of these features. Since it has no operating system on the Arduino, it is essentially just a processing unit that needs to be programmed by the user. Even while all of these functions may be added, an Arduino's computing power is substantially lower than a Raspberry Pi's. This would severely restrict the project's ability to use, for example, a graphical user interface or the internet to handle data.

11.4.6.2 *Intel Edison*

Due in part to the fact that we already had access to Raspberry Pi devices that met all the requirements; these weren't seriously considered as alternatives. The fact that tablets, smartphones, and Edison are either unsuitable for this type of project or either too expensive or difficult to use is another problem. A smartphone or tablet might likely be used to interface with the final system in the future, but using them as part of the system at this time would simply be impractical owing to their complexity.

11.4.6.3 *Raspberry Pi*

The Raspberry Pi was designed to be something that all other electronics could connect to and that would send all incoming data to NR for additional routing. This objective was accomplished since every tested external device could establish a wired or wireless connection with the Raspberry Pi. These included a keyboard, a seven-inch LCD touch screen for the Raspberry Pi, and a USB Wi-Fi dongle. Some of these accessories, like the RFID reader, are required for the system to function, while others, like the Wi-Fi dongle, are optional. The Raspberry Pi functioned well in its function as the main hub for the other devices, and it showed no signs of being overloaded or having trouble processing all the data flowing through it. There would be no need for a USB extension hub owing to the four available USB ports. It was also relatively simple to create the GUI due to the ability to run high-level scripts.

The Raspberry Pi does not come with an operating system. For it, you need New Out of the Box Software, sometimes referred to as NOOBS. With the help of this system management, installing, setting up, and configuring your Raspberry Pi is a breeze. Several OS are available when NOOBS first starts up for your selection [21]. Table 11.1 shows the specification of various systems and by the system we can see how the Raspberry Pi model is the best to be utilized for the purpose of monitoring system.

Table 11.1 Specification Comparison of Various Systems

<i>Name</i>	<i>Intel Edison</i>	<i>Raspberry Pi 3</i>	<i>Arduino</i>
CPU Clock frequency	500 MHz	1.4 GHz	16 MHz
RAM	1 GB	1 GB	2 KB
Flash Storage	4 GB	8 GB	32 KB
Ethernet Port	-	Yes	-
Wi-Fi	Yes	Yes	-
Bluetooth	Yes	Yes	-
USB Connectivity	-	4	-
GPU	-	Yes	-
Audio	-	3.5 mm	-
GPIO/ Pins	12	40	14
Reference	16	15	17

The available operating systems depend on the type of Raspberry Pi you are using. We will stick to the most popular operating systems that can be found on the latest Raspberry Pi devices for the purposes of this chapter. At the moment, that included RISC OS, Open ELEC, Raspbian, Windows, IoT Core, and OSMC.

11.5 Result and Discussion

This section deals about the results and the discussion. When receiving the sensor information and upgrading it on the website in the suggested system, application software is crucial. Raspberry Pi 3 is the primary piece of software utilized here. Raspberry Pi 3 is a lodged scheduling policy that holds up a range of microprocessors and gives them access to a full application framework. Figure 11.3 depicts the model used for forecasting heart attacks.

In the proposed work probability of heart attack is predicted using record of 60 patients using four models i.e., Simple Linear Regression Model, KNN Model, Support Vector Machine (SVM) using RBF kernel, and Gaussian Naïve Bayes models and results for linear regression model and KNN model is shown using Figure 11.4. In Figure 11.4, the violate line represents the actual value and red bullet represents the predicted value.

Several machine learning algorithms are used to evaluate the model for heart attack prediction using the ECG output data collected from the AD8232 sensor.

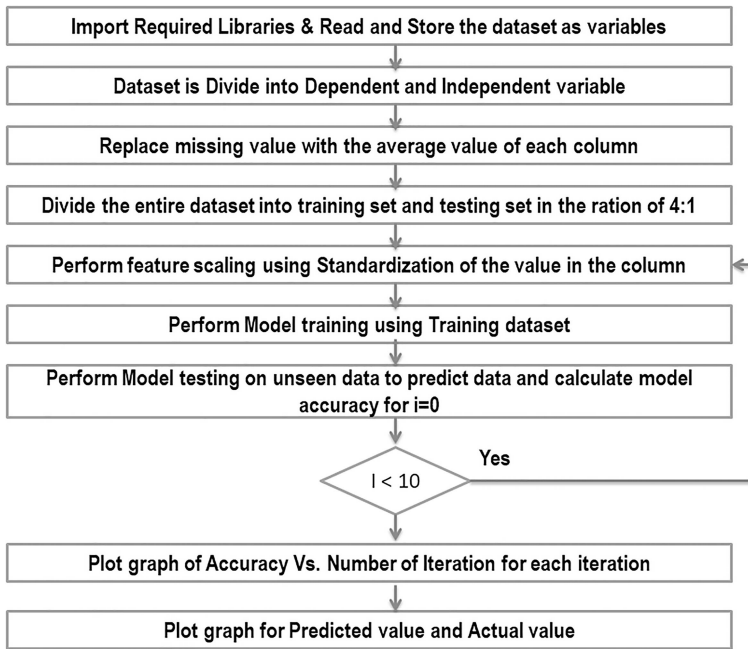


Figure 11.3 Heart attack forecasting system.

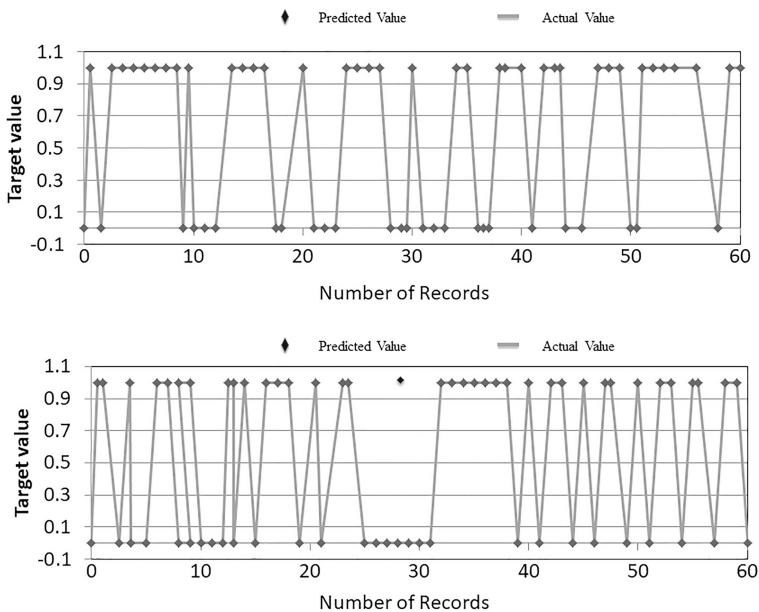


Figure 11.4 Comparison between simple linear regression and KNN model.

The dataset contains 60 entries. Figure 11.5 shows a graph comparing the dependent variable (Y test) to the values predicted using SVM and Gaussian Naïve Bayes models (Y predicts).

Table 11.2 shows the performance comparison with Dwivedi [22] and Shah et al. [23] and the table shows that the SVM with RBF kernel shows the highest

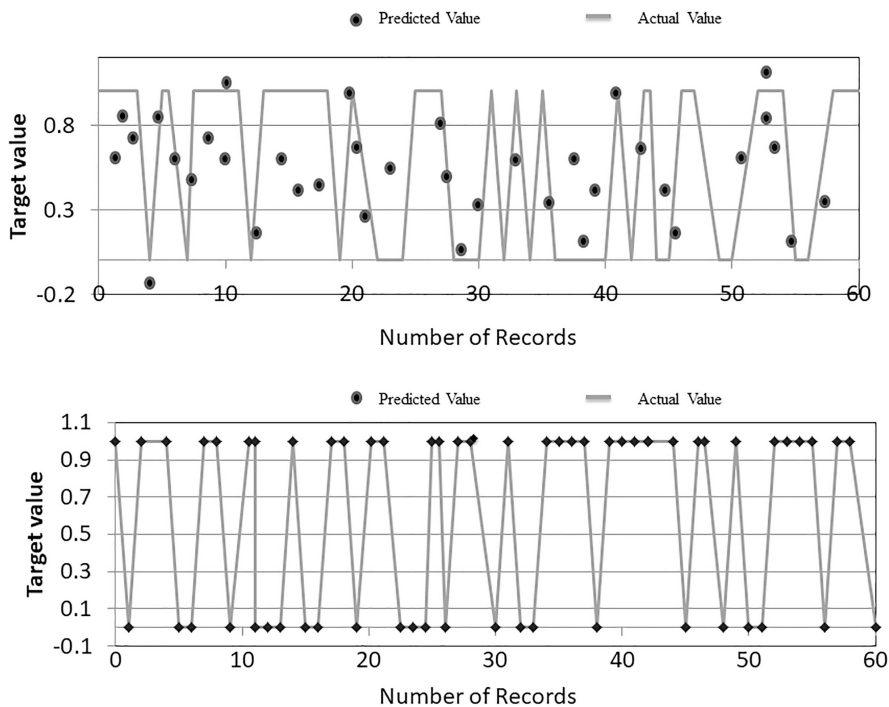


Figure 11.5 Comparison of SVM and Gaussian Naïve Bayes.

Table 11.2 Performance Comparison with [22] and [23]

Classifier	Dwivedi, 2018 [22]	Shah et al., 2020 [23]	Proposed
Simple Linear Regression (SLR)	85%	70%	47.5%
K Nearest Neighbor (KNN)	80%	90.78%	45%
Gaussian Naive Bayes	83%	88.15%	55%
SVM (RBF Kernel)	82%	84%	90%

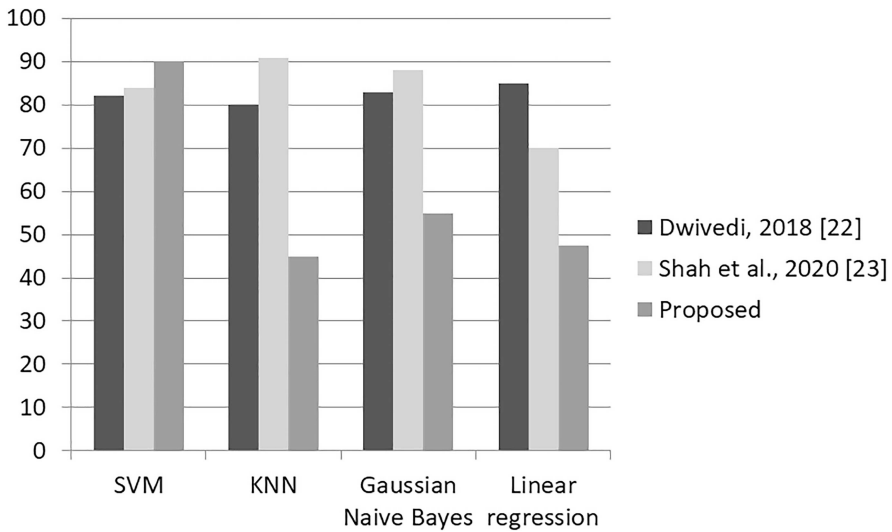


Figure 11.6 Performance comparison with [22] and [23].

level of accuracy of 90% as compared to [22] and [23]. The bold value shows the superior performance over other models.

Figure 11.6 shows the comparison with the performance of four machine learning models with [22] and [23] and it clearly shows that SVM with RBF kernel performs well and gives accuracy of 90% as compared to other models. The reason behind the good performance of the SVM is its good ability to predict the value using various kernel methods.

11.6 Conclusion and Future Scope

The sensors are effectively connected in order to collect the data on the vital signs, and the information is then precisely delivered to the Amazon server. The accuracy of the broadcast and received signals was determined by comparison. Additionally, a GSM module is employed to inform the user in case of irregularities in vital signs. With the use of machine learning algorithms and the relevant dataset, the heart attack prediction model is also put into practice and it is found that RBF SVM classifier shows the maximum classification accuracy of 90%. In future different models or deep learning models can be used for the prediction of heart attack.

References

1. Bourouis, A., Feham, M., & Bouchachia, H. (2011). Ubiquitous Mobile Health Monitoring System for Elderly (UMHMSE). *International Journal of Computer Science and Information Technology* 3. 10.5121/ijcsit.2011.3306.

2. Ramkumar, G., Seetha, J., Priyadarshini, R., Gopila, M., & Saranya, G. (2023). IoT-Based Patient Monitoring System for Predicting Heart Disease Using Deep Learning. *Measurement, Science Direct* 218. 10.1016/j.measurement.2023.113235.
3. Sahoo, S., Borthakur, P., Baruah, N., & Chutia, B. P. (2021). IoT and Machine Learning Based Health Monitoring and Heart Attack Prediction System. *Journal of Physics: Conference Series*. 10.1088/1742-6596/1950/1/012056.
4. Brown, T. (2022). In Patients Come Second, Health Care Workers Come First. *American Journal of Nursing*. 10.1097/01.NAJ.0000833924.89861.73.
5. Mendhe, N. M., Sharmila, D., & Ramesh, M. (2022). Artificial Intelligence-Based Web-Centric E-health Monitoring System. 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2022, pp. 1–5. 10.1109/ICSES55317.2022.9914101.
6. Bhowmik, T., Mojumder, R., Banerjee, I., & Das, G. (2021). IoT Based Data Aggregation Method for E-Health Monitoring System. 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 1–7. 10.1109/ICCCNT51525.2021.9579885.
7. Anshu, S., Moghe, A. A., & Agarwal, R. (2022). Advance sensing in image processing and IoT. In: *IoT for Health Monitoring*. CRC Press. 10.1201/9781003221333-11.
8. Keerthana, N., Lokeshwaran, K., Kavinkumar, P. S., Kaviyan, T., Manimaran, M., & Elango, S. (2021). Fingerprint Integrated E-Health Monitoring System Using IoT. In: Arunachalam, V., Sivasankaran, K. (Eds.), *Microelectronic Devices, Circuits and Systems*. ICMDCS 2021. Communications in Computer and Information Science, vol 1392. Springer. 10.1007/978-981-16-5048-2_12.
9. Tinetti, M., Dindo, L., Smith, C. D., Blaum, C., Costello, D., Ouellet G., et al. (2019). Challenges and Strategies in Patients' Health Priorities-Aligned Decision-Making for Older Adults with Multiple Chronic Conditions. *PLoS One* 14(6): e0218249. 10.1371/journal.pone.0218249.
10. Haleem, A., Javaid, M. D., Singh, P. R., & Suman, R. (2022). Medical 4.0 Technologies for Healthcare: Features, Capabilities, and Applications. *Internet of Things and Cyber-Physical Systems* 2. 10.1016/j.iotcps.2022.04.001.
11. Dash, S., Shakyawar, S. K., Sharma, M. et al. (2019). Big Data in Healthcare: Management, Analysis and Future Prospects. *Journal of Big Data* 6: 54. 10.1186/s40537-019-0217-0.
12. Davis, M. W., Kirwan, M. J., Maclay, W. N., & Pappas, H. P. (Eds.). (2022). *Closing the Care Gap with Wearable Devices: Innovating Healthcare with Wearable Patient Monitoring*. CRC Press.
13. Bagga, T., Upreti, K., Kumar, N., Ansari, A. H., & Nadeem, D. (Eds.). (2022). *Designing Intelligent Healthcare Systems, Products, and Services Using Disruptive Technologies and Health Informatics*. CRC Press.
14. Chou, H.-M., Pi, S.-M., & Cho, T.-L. (2022). An Intelligent Healthcare System for Residential Aged Care during the COVID-19 Pandemic. *Applied Sciences* 12(22): 11847. 10.3390/app122211847.
15. Khang, A., Rana, G., Tailor, R. K., & Abdullayev, V. (Eds.). (2023). *Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem*. CRC Press.
16. Liu, J., Liu, M., Bai, Y., Zhang, J., Liu, H., & Zhu, W. (2020). Recent Progress in Flexible Wearable Sensors for Vital Sign Monitoring. *Sensors* 20(14): 4009. 10.3390/s20144009.

17. Sharma, A., Badea, M., Tiwari, S., & Marty, J. L. (2021). Wearable Biosensors: An Alternative and Practical Approach in Healthcare and Disease Monitoring. *Molecules* 26(3): 748. 10.3390/molecules26030748.
18. Das, A., Nayeem, Z., Faysal, A. S., Himu, F. H., & Siam, T. R. (2021, March). Health Monitoring IoT Device with Risk Prediction Using Cloud Computing and Machine Learning. In 2021 National Computing Colleges Conference (NCCC). pp. 1–6. IEEE. 10.1109/NCCC49330.2021.9428798.
19. Ahamed, S., Bhatt, P., Sultanuddin, S. J., Walia, R., Haque, M. A., & InayathAhamed, S. B. (2022, January). An Intelligent IoT Enabled Health Care Surveillance Using Machine Learning. In 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). pp. 1–5. IEEE. 10.1109/ACCAI53970.2022.9752648.
20. Gawali, M. K., & Rambabu, C. (2021, May). IoT Model for Heart Disease Detection Using Machine Learning (ML) Techniques. In *Techno-Societal 2020: Proceedings of the 3rd International Conference on Advanced Technologies for Societal Applications—Volume 1* pp. 399–409. Springer International Publishing. 10.1007/978-3-030-69921-5_41.
21. Almujally, N. A., Aljrees, T., Saidani, O., Umer, M., Faheem, Z. B., Abuzinadah, N., & Ashraf, I. (2023). Monitoring Acute Heart Failure Patients Using Internet-of-Things-Based Smart Monitoring System. *Sensors* 23(10): 4580. 10.3390/s23104580.
22. Dwivedi, A. K. (2018). Performance Evaluation of Different Machine Learning Techniques for Prediction of Heart Disease. *Neural Computer Applications* 29(10): 685–693. 10.1007/s00521-016-2604-1.
23. Shah, D., Patel, S., & Bharti, S. K. (2020). Heart Disease Prediction Using Machine Learning Techniques. *SN Computer Science* 1(6). 10.1007/s42979-020-00365-y.

Chapter 12

Challenges of Image Processing-Based Applications in the Analytics of Internet of Things

Mohammad Idrees Bhat¹, Arif Mohammad Lattoo²,
and Shubhalaxmi Joshi¹

¹*School of Computer Science, MIT-World Peace University, Pune, Maharashtra, India*

²*Sonata Software Limited, Bangalore, Karnataka, India*

12.1 Introduction

With the rapid advancements in internet technologies, including image processing/analysis, cloud computing, analytics of BigData, and many more, we are witnessing exponential applications for the analytics of Internet of things (IoT), in order to, process BigData streams. In fact, image processing (IP) based IoT applications have been regarded as an utmost important. Because of their real-time applications, such as smart-cities, devices, vehicles, and people. Moreover, they also carry tremendous amount of applications in monitoring of health, behavior, manufacturing, traffic, and atmospheric conditions, etc. Furthermore, IoT analytics is extensively used in entertainment (multi-media), agriculture, and medicine industries irrespective of

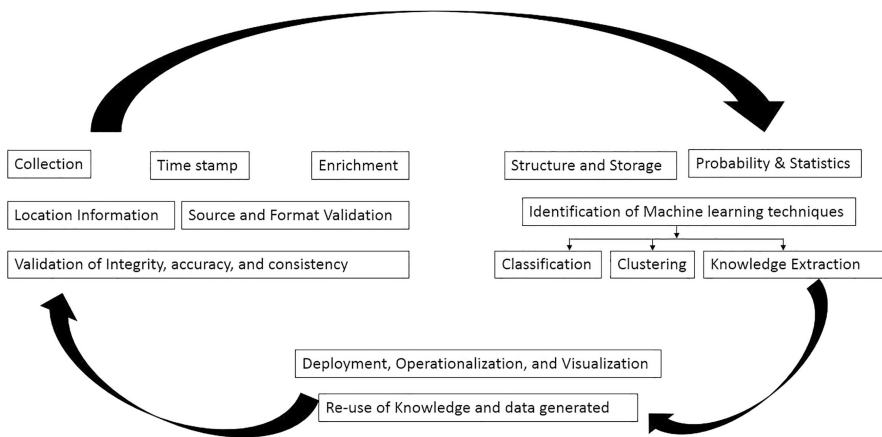


Figure 12.1 Illustration of Internet of Things (IoT) life cycle.

geographical location by incorporating technology based on remote sensing and drones. As a result, integration of image processing and IoT offers capacity, fault tolerance, performance, and scalability to applications. Considering this business potential, there is limited research in investigating challenges and issues in this integration at the outset (Kumar et al., 2022; Manyika et al., 2015). Therefore, it is indispensable to first identify and understand challenges later find suitable and proper solutions for their efficient design, development, operation, and deployment.

In general, IoT analytics life cycle is categorized into following: (i) data collection, (ii) data analysis, and (iii) re-use (Figure 12.1). In **collection stage**, data is enriched, transformed, time stamped, and validated, in order to, ensure format, origin, integrity, accuracy, and consistency of the data. For this reason, various middleware, data management, and interoperability techniques/devices are used. Consequently, more challenges get accumulated in this stage. **Data analysis stage** comprises of structuring, storage, and analysis, such that, proper insights can be inferred for decision making. Strictly speaking, this stage mainly comprises machine learning/deep learning, knowledge modeling, probability, statistics, data-mining, management, and association, etc. based techniques. Finally, **re-use stage** makes IoT applications operationalize (Chen & Wu, 2021; Guillen, 2019; Gupta et al., 2022; Soldatos, 2017; Surya et al., 2022).

In standard IoT architecture (Figure 12.2), the role of image processing becomes important and indispensable in data collection stage/sensor/perceptron stage and service/process layers, respectively. For example, at sensor layer, various camera-based sensors are installed to collect/perceive the real-time data for different applications. Afterwards, this real-time data is continuously transmitted through data transformation layer/network layer (via both cloud and physical) to data process layer/service layer where this image data is processed/analyzed to get insights and subsequently presented at presentation/application layer.

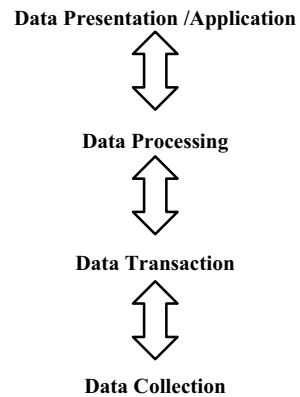


Figure 12.2 Typical Internet of Things (IoT) architecture.

In literature (Abdel Magid et al., 2020; Diana & Millet, 2021; Gupta et al., 2022; Ryan et al., 2013; Sharma et al., 2020; Surya, 2022), IoT data streams are considered as BigData. As a matter of fact, as they come with huge volume and velocity, greater variety, and veracity. As a result, further complexities of BigData get involved in this integration. In the next section, we categorized challenges of image processing-based applications in the analytics of IoT considering the BigData characteristic in view.

12.2 Challenges of Image Processing-Based Applications in Internet of Things (IoT) Analytic

12.2.1 Heterogeneity

In general, image data may differ in format, volume, semantics, modality, and dimension. Thanks to different and diverse hardware architectures, operating systems, application software and gateway requirements (Atanasova, 2019). Consequently, impreciseness, uncertainties and incompleteness occur in heterogeneous data. As a matter of fact, numerous studies (Atanasova, 2019; Brooks & Grigsby, 2013; Devin Miles, 2020; Sethi & Sarangi, 2017; X. Wang et al., 2023; Zhong et al., 2018), deal with the quantification of this heterogeneity. For example, in (Moshinsky, 2020), position emission tomography computed tomography (PET-CT), and position emission tomography magnetic resonance imaging (PET-MRI).

Furthermore, in most of the cases classification of image is viewed from multiple information cues. Therefore, image data expose every IoT application with the data variety, veracity, volume, and velocity at the outset. In addition, assembling/integrating this heterogeneous BigData requires up-to-date connectors and drivers. More importantly, IoT applications have to understand semanticity of these diverse data streams in real-time as well. Overall, processing of heterogeneous data with stated ambiguities gets extremely challenging in complex IoT applications.

12.2.2 Varying Quality

Image data quality is one of the challenging issues in an entire domain of computer vision and image processing in general and in IoTs in particular. As the capturing of images are not following any pre-defined criteria, therefore, images get clicked/captured in different lighting conditions, angles, and dots per inch (DPI). Due to this noisy, unreliable, and incomplete data, various issues and uncertainties arise in IoT applications (Ryan et al., 2013). Different techniques and procedures are needed to remove these uncertainties. For example, binarization, removal of noise and skewness, rescaling and changing morphology of images as per the demands in IoT applications. We can have an idea of data quality from (Defeo, 2017; Liu et al., 2020; R. Y. Wang et al., 2013), where it is described as ready to fit and conformance to requirements for the applications.

12.2.3 Real-Time Nature

As stated, IoT applications expect high velocity of data, therefore, there is a need for real-time processing of the data. Additionally, with the rapid advancements in machine and deep learning technologies, the real-time processing of image data has increased demands for high-end hardware requirements also. For instance, in applications which deal with the image processing in smart factories for monitoring the conditions of machinery, control over the inventory of raw materials, real-time identification of anomalies and abnormalities in medical image data. Furthermore, real-time automatic license plate recognition for identifying traffic rule violator (Chen & Wu, 2021), etc. Overall, there is need for the sophisticated hardware and environment whose focus should be capturing any abrupt change in the data patterns, in order to, fulfill the real-time processing demands.

12.2.4 Time and Location

Almost all IoT applications have to process data streams with temporal and spatial context. With respect to image processing-based applications, this feature becomes more prominent and indispensable. In addition, in many IoT applications data streams need to be dynamically filtered and selected for analytic purpose (Ryan et al., 2013). For example, in wild-life monitoring, traffic control systems, bio-medical field, and many more. Therefore, high-end software and hardware are required for achieving these features. Such as cloud, edge, and sensing architectures.

12.2.5 Privacy and Security

As image data streams are ubiquitous and distributive in nature addressing privacy and security concerns are utmost important. For instance, in healthcare IoT applications large volume of image data need high-end encryption-decryption and privacy preservation algorithms in order to secure data and thwart malicious attacks.

12.2.6 Bias

In general, artificial intelligence and machine learning (AI&ML) revolve around data and, in particular, for functioning of IoT applications it is everything. Hence, at first, data must be distilled for quality, in order to, meet functional standards. Currently, AI&ML models in computer vision are built after partition the image data into training, validation, and testing sets, respectively. For instance, in categorization/classification of images, identification and segmentation of pre-defined objects, etc. To accomplish these objectives efficiently and smoothly image data must be reliable. Therefore, the use of all the techniques of AI&ML for this purpose comes into play in IoT applications.

12.3 Conclusion

This chapter, at first, has outlined the role of image processing (IP) in the analytics of internet of things (IoTs) and presented some related technologies and applications, Such as smart monitoring of wild-life, agriculture, traffic control, and bio-medical. The rest of the chapter is devoted in categorizing these challenges that arise in this integration (IP and IoTs) that stems from the characteristics and nature of image data.

References

- Abdel Magid, S., Petrini, F., & Dezfouli, B. (2020). Image classification on IoT edge devices: Profiling and modeling. *Cluster Computing*, 23(2), 1025–1043. 10.1007/s10586-019-02971-9
- Atanasova, T. (2019). Methods for processing of heterogeneous data in IoT based systems. *Communications in Computer and Information Science*, 1141 CCIS (December), 524–535. 10.1007/978-3-030-36625-4_42
- Brooks, F. J. & Grigsby, P. W. (2013). Quantification of heterogeneity observed in medical images. *BMC Medical Imaging*, 13(1), 1–12. 10.1186/1471-2342-13-7.
- Chen, M. Y., & Wu, H. Te. (2021). Real-time intelligent image processing for the Internet of Things. *Journal of Real-Time Image Processing*, 18(4), 997–998. 10.1007/s11554-021-01149-0
- Defeo, J. A. (2017). *Juran's Quality Handbook: The Complete Guide to Performance Excellence*. 7th edn. McGraw-Hill Education, New York.
- Diana, M. J., & Millet, P. (2021). Towards ubiquitous low-power image processing platforms. In *Towards Ubiquitous Low-power Image Processing Platforms*. 10.1007/978-3-030-53532-2
- Guillen, G. (2019). Sensor projects with Raspberry Pi. In *Sensor Projects with Raspberry Pi*. Apress. 10.1007/978-1-4842-5299-4
- Gupta, R., Rana, A. K., Dhawan, S., & Cengiz, K. (2022). *Advanced Sensing in Image Processing and IoT* (Vol. 21, Issue 1). <http://journal.umsurabaya.ac.id/index.php/JKM/article/view/2203>

- Kumar, N., Kumar, K., & Kumar, A. (2022). Application of Internet of Things in Image Processing. *2022 IEEE Delhi Section Conference, DELCON 2022*. 10.1109/DELCON54057.2022.9753308
- Liu, C., Nitschke, P., Williams, S. P., & Zowghi, D. (2019). Data quality and the Internet of Things. *Computing*, 102(2), 573–599. 10.1007/s00607-019-00746-z.
- Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). The Internet of Things: Mapping the value beyond the hype. *McKinsey Global Institute, June (2015), June*, 719–746. 10.4018/978-1-7998-9155-0.ch036
- Moshinsky, M. (2020). Significance of Image Heterogeneity in Multi-Modality Medical Imaging. *Nuclear Physics*, 13(1), 104–116.
- Ryan, C., & Tauer. (2013). Building Blocks for IoT Analytics. In *Paper Knowledge. Toward a Media History of Documents*, River Publishers Series in Signal, Image, and Speech Processing.
- Significance of Image Heterogeneity in Multi-Modality Medical Imaging January 26 (2017). *Devin Miles with David Jordan*.
- Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 1–25. .10.1155/2017/9324035
- Sharma, A., Singh, P. K., & Kumar, Y. (2020). An integrated fire detection system using IoT and image processing technique for smart cities. *Sustainable Cities and Society*, 61(December 2019), 102332. 10.1016/j.scs.2020.102332
- Soldatos, J. (2017). *Building Blocks for IoT Analytics*. 10.13052/rp-9788793519046
- Surya, T., Chitra Selvi, S., & Selvaperumal, S. (2022). The IoT-based real-time image processing for animal recognition and classification using deep convolutional neural network (DCNN). *Microprocessors and Microsystems*, 95(September), 104693. 10.1016/j.micpro.2022.104693
- Wang, R. Y., Strong, D. M., Wang, R. Y., & Strong, D. M (2013). *Beyond Accuracy?: What Data Quality Means to Data Consumers*, 12(4), 5–33.
- Wang, X., Chen, W., Xia, J., Wen, Z., Zhu, R., & Schreck, T. (2023). HetVis: A Visual analysis approach for identifying data heterogeneity in horizontal federated learning. *IEEE Transactions on Visualization and Computer Graphics*, 1–10. 10.1109/tvcg.2022.3209347
- Zhong, F., Chen, Z., Ning, Z., Min, G., & Hu, Y. (2018). Heterogeneous visual features integration for image recognition optimization in Internet of Things. *Journal of Computational Science*, 28, 466–475. 10.1016/j.jocs.2016.11.002.

Chapter 13

Internet of Things for Smart Agricultural Practices

Wasswa Shafik^{1,2}, Ali Tufail¹,
Rosyzie Anna Awg Haji Mohd Apong¹, and
Liyanage Chandratilak De Silva¹

¹*School of Digital Science, Universiti Brunei Darussalam, Bandar Seri Begawan, Brunei Darussalam*

²*Dig Connectivity Research Laboratory (DCRLab), Kampala, Uganda*

13.1 Introduction

Internet of Things (IoT), networks of interconnected devices, sensors, and systems capable of collecting and exchanging data over the Internet. These devices, equipped with sensors and actuators, communicate with each other and centralized platforms to enable seamless data sharing and real-time decision-making [1]. IoT encompasses many technologies, including sensors, wireless communication, cloud computing, and data analytics, all working together to enable intelligent connectivity and automation. The advent of the IoT has brought forth a transformative wave of technological advancements across various industries, and the agricultural sector is no exception. IoT has opened up new avenues for innovation, particularly in Smart agriculture [2]. This introduction provides a comprehensive overview of the topic, starting with the definition of IoT, followed by an exploration of smart agriculture and the significance of incorporating IoT in agricultural practices.

Smart agriculture, precision agriculture, or digital farming, is an innovative approach that leverages technology to optimize agricultural practices and enhance productivity while minimizing resource wastage. It involves the integration of IoT devices and systems into various agricultural processes, enabling farmers to monitor and manage their crops, soil, livestock, and environmental conditions with greater precision and efficiency [3]. Smart Agriculture utilizes advanced technologies such as sensors, drones, satellite imagery, and data analytics to gather and analyze real-time data, providing farmers with actionable insights to make informed decisions and optimize their farming operations.

The application of IoT in agriculture holds immense importance and offers numerous benefits to farmers and the agricultural industry as a whole. Farmers can achieve greater efficiency, productivity, and sustainability by integrating IoT devices and systems into agricultural practices [4]. IoT-enabled sensors can monitor critical parameters like temperatures, soil moisture, potential hydrogen (pH) levels, and crop health, enabling farmers to make data-driven irrigation, fertilization, and pest control decisions. This precision and optimization lead to higher crop yields and minimize the use of water, fertilizers, and pesticides, contributing to environmental conservation and cost reduction [5].

IoT in architecture is mainly layered into three, as presented in Figure 13.1. First, the perception Layer collects data from physical devices or sensors embedded in the environment. It includes devices such as sensors, actuators, cameras, and other data-gathering mechanisms that capture information from the real world. Network Layer facilitates the communication and transfer of data between the perception layer and the higher layers of the IoT architecture. It encompasses protocols, gateways, routers, and other networking components that enable connectivity and data transmission over local or wide-area networks. Lastly, the application layer is the topmost layer of

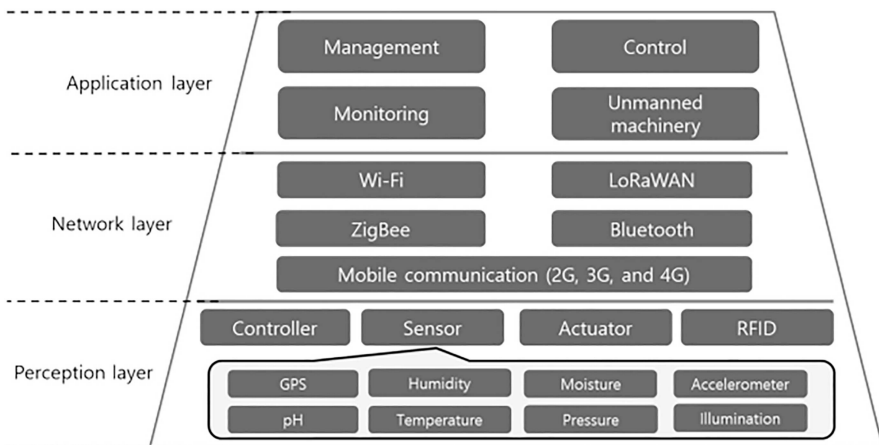


Figure 13.1 Traditional Internet of Things architecture.

the IoT architecture, where data is utilized to derive meaningful insights and enable various applications and services. It encompasses software applications, user interfaces, analytics tools, and other services that leverage the collected data to provide valuable functionality, automation, and decision-making capabilities for end-users or other systems.

IoT-based automation and control systems, for example, smart irrigation and autonomous farming equipment, improve operational efficiency and reduce labor requirements. Furthermore, IoT in agriculture facilitates real-time monitoring and remote management, allowing farmers to monitor their fields and livestock anywhere. This remote access enhances convenience, enables proactive response to potential issues, and helps in the early detection of diseases or anomalies, minimizing losses and improving overall farm management [6]. Moreover, IoT-driven data analytics and predictive models enable farmers to gain valuable insights into market trends, consumer preferences, and supply chain management, aiding in informed decision-making and optimizing farm-to-fork processes.

The growing need for sustainable and efficient farming practices to meet global food security challenges drives the widespread adoption of IoT technology in the agricultural sector. With a rapidly expanding population, it is estimated that food production will necessitate an increase of 70% by 2050. IoT offers a promising solution by enabling agriculturists to optimize agricultural processes and make data-driven decisions. In real-time, farmers can monitor and analyze crucial parameters like weather conditions, nutrient levels, crop health, and soil moisture by incorporating IoT sensors into farming operations [7]. This continuous data collection provides valuable insights and enables farmers to implement targeted actions and interventions. For example, farmers can adjust irrigation schedules based on soil moisture data, apply fertilizers precisely where needed, and identify and mitigate potential pest and disease outbreaks early on.

One of the significant advantages of IoT in agriculture is its ability to improve resource management. By optimizing water usage through smart irrigation systems and monitoring weather conditions, farmers can minimize water wastage while ensuring that crops receive adequate moisture through real-time implementation, as demonstrated in Figure 13.2. This leads to significant water conservation and cost savings. Similarly, IoT-enabled precision farming techniques help optimize fertilizers and pesticides, reducing environmental impact and input costs. In addition to crop monitoring, IoT plays a vital role in livestock management [8]. Connected devices such as animal tracking systems and health monitoring sensors enable farmers to monitor livestock's location, behavior, and health. This information facilitates better decision-making, such as adjusting feeding schedules, identifying signs of illness, and improving overall animal welfare.

The benefits of IoT in agriculture extend beyond individual farms. With the help of IoT-enabled data analytics and predictive models, farmers can gain insights into market trends, consumer preferences, and supply chain optimization. This allows for improved decision-making regarding crop selection, production

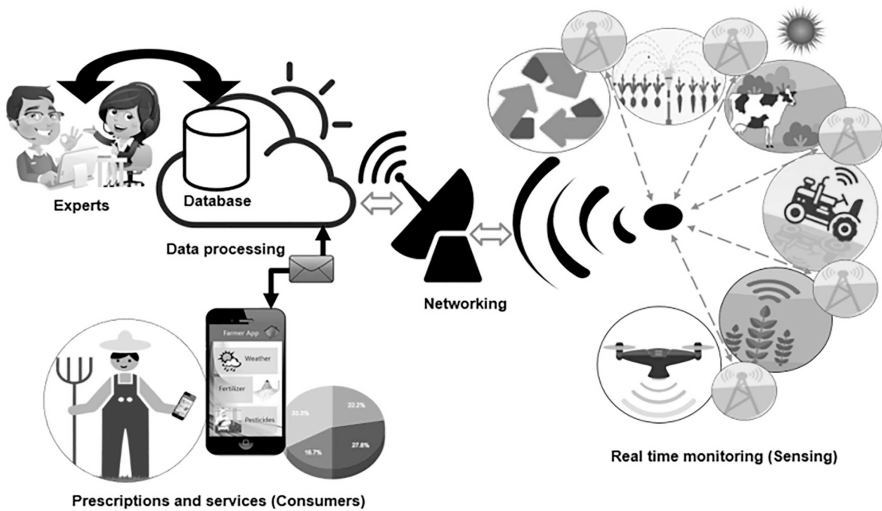


Figure 13.2 A sample procedure of agricultural IoT application from consumer experts to real-time monitoring [9].

planning, and efficient distribution of agricultural products, ultimately benefiting the entire agricultural value chain.

Overall, incorporating IoT in agriculture holds tremendous potential for transforming traditional farming practices into smart, data-driven systems. By leveraging IoT technologies, farmers can optimize resource usage, improve productivity, reduce environmental impact, and contribute to global food security [10]. The subsequent sections will delve deeper into the specific applications and advancements in IoT for smart agriculture.

13.1.1 The Contribution of the Chapter

The chapter presents the following contributions:

- Provides an overview of IoT's applications in the agricultural sector, specifically focusing on smart agriculture.
- Highlights the importance and benefits of implementing IoT in agriculture.
- Identifies various IoT sensors and devices used for soil, crop, and livestock monitoring in smart agriculture and discusses data collection techniques for gathering agricultural data, including wireless sensor networks and remote sensing technologies.
- Explores data analytics and processing methods, such as cloud computing and edge computing, for analyzing agricultural data and making informed decisions.
- Examines automation and control systems in smart agriculture, including smart irrigation, precision farming, and livestock management.

- Discusses connectivity and communication technologies, such as Wi-Fi, cellular networks, and LPWAN, for seamless data transmission in IoT-enabled agriculture systems.
- Addresses data security and privacy considerations in the implementation of IoT in agriculture.
- Presents case studies and success stories of successful IoT implementations in smart agriculture and identifies future trends and challenges in IoT-enabled smart agriculture, including integration with emerging technologies like blockchain and AI, scalability, interoperability, and standardization.
- Finally, emphasizing IoT's potential impact and growth opportunities in smart agriculture calls for further research and implementation of IoT for improved productivity and sustainability.

13.1.2 The Chapter Organization

The remainder of this chapter is structured in seven sections. Section 13.2 presents IoT sensors and devices as they are used in smart agriculture, including soil, crop, and livestock monitoring, for example, soil moisture sensors, pH sensors, temperature sensors, animal tracking devices, weather sensors, health monitoring sensors, feed monitoring systems, nutrient level sensors, crop health sensors among others. Section 13.3 demonstrates data collection and analysis like predictive analytics and decision support systems data-gathering techniques, data analytics, and processing. Section 13.4 illustrates automation and control systems, smart irrigation, precision farming, and livestock management; these approaches include automated irrigation systems and water management and optimization, variable rate technology and autonomous farming equipment, machine learning algorithms, and artificial intelligence applications. Section 13.5 presents connectivity and communication aspects of smart agriculture, like wireless communication technologies, data security, and privacy considerations like encryption and authentication, data ownership, and access control. Section 13.6 presents selected case studies of smart farming using IoT, entailing examples of successful IoT implementations in smart agriculture and the benefits farmers and agricultural enterprises achieve. Section 13.7 holds the Future trends and challenges like integrating with other emerging technologies (for instance, blockchain, AI), scalability and interoperability, standardization, and regulatory considerations, among others. Finally, Section 13.8 presents brief lessons learned and the conclusion of the chapter.

13.2 IoT Sensors and Devices for Smart Agriculture

IoT sensors and devices have become indispensable tools in smart agriculture, revolutionizing traditional farming practices and enabling precision agriculture. These sensors and devices play a critical role in collecting and transmitting real-time

data about various agricultural parameters, empowering farmers with actionable insights to optimize their farming operations. From soil monitoring to crop health and livestock management, IoT sensors and devices offer numerous applications that enhance productivity, resource efficiency, and sustainability in smart agriculture. This section demonstrates the top three sensors and devices that aid smart farming.

13.2.1 Soil Monitoring

IoT sensors provide invaluable information about crucial soil parameters such as moisture levels, pH balance, and temperature in soil monitoring. Soil moisture sensors enable farmers to precisely monitor and manage irrigation, preventing overwatering and underwatering, which can significantly impact crop growth and yield [11]. By continuously monitoring the soil's moisture content, these sensors provide real-time data that informs irrigation decisions, resulting in optimal water usage and enhanced crop health.

13.2.1.1 Soil Moisture Sensors

With IoT-enabled soil moisture sensors, farmers can continuously monitor the moisture levels in the soil in real-time. These sensors provide accurate and timely data transmitted wirelessly to a centralized platform for analysis and decision-making. By accessing this information remotely, farmers can determine the exact water requirements of their crops and optimize irrigation practices accordingly, ensuring that the soil moisture remains within the ideal range. This targeted approach minimizes water wastage, prevents over- or under-watering, and promotes optimal crop growth and health [12]. Additionally, IoT enables farmers to set up automated irrigation systems that can be controlled and monitored remotely, providing further flexibility and efficiency in water management [13]. Overall, IoT-enabled soil moisture sensors facilitate precise irrigation management, improving water conservation, enhanced crop productivity, and sustainable farming practices, as Figure 13.3 depicts a summary of IoT applications to enhance agriculture.

13.2.1.2 Soil pH Sensors

With IoT-enabled soil pH sensors, farmers can continuously measure and monitor the acidity or alkalinity levels of the soil in real-time. These sensors provide accurate and timely data transmitted wirelessly to a central system for analysis and decision-making. By accessing this information remotely, farmers can determine the pH status of the soil and make informed decisions regarding soil amendments and fertilization practices. This targeted approach ensures that the soil pH remains within the optimal range for specific crops, facilitating nutrient availability and uptake [14]. As a result, farmers can prevent nutrient deficiencies or toxicities by maintaining the ideal pH balance, optimizing nutrient utilization, and promoting healthy plant growth.

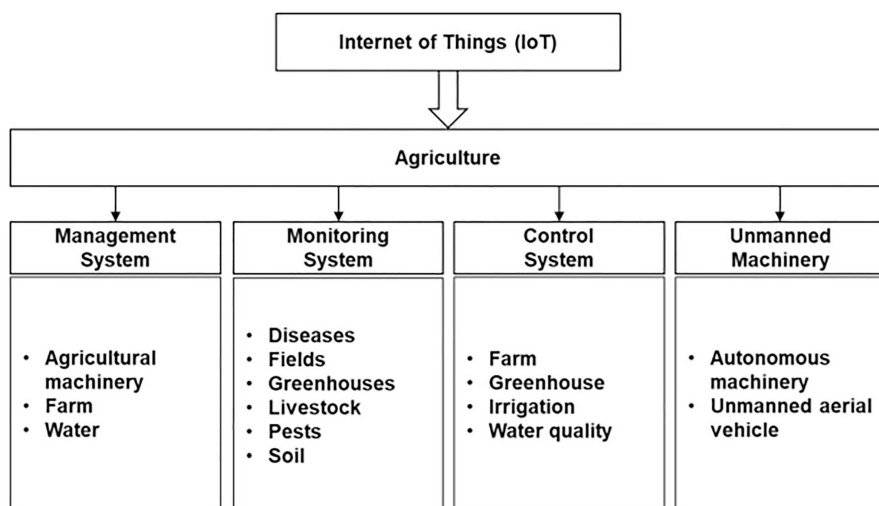


Figure 13.3 Agricultural Internet of Things (management, monitoring, control, and unmanned (automatic) systems).

IoT-enabled soil pH sensors offer a cost-effective and efficient solution for precision soil monitoring, letting agriculturists achieve optimal soil conditions and make data-driven decisions for improved agricultural outcomes.

13.2.1.3 Soil Temperature Sensors

Farmers can make informed decisions regarding planting schedules, irrigation management, and nutrient application by monitoring soil temperature. Soil temperature impacts seed germination, root development, microbial activity, and nutrient availability, among other crucial factors for plant growth. By leveraging IoT technology, farmers can monitor soil temperature variations and adjust their farming practices accordingly, ensuring that the soil temperature remains within the desired range for specific crops. This targeted approach promotes optimal crop growth, reduces the risk of plant stress or diseases related to extreme temperatures, and facilitates effective resource allocation for sustainable soil management [15]. IoT-enabled soil temperature sensors offer a valuable tool in precision agriculture, enabling farmers to make data-driven decisions and maximize the productivity and health of their crops.

13.2.2 Crop Monitoring

Crop monitoring, in the context of Smart Agriculture and IoT, refers to the continuous and real-time observation of crops using various sensors and technologies. IoT-enabled devices, such as spectral imaging, infrared sensors, and drones, are

deployed to gather data on crop health, growth, nutrient levels, and environmental conditions. This data is then analyzed and used to make informed decisions, enabling farmers to optimize crop management practices, detect early signs of stress or disease, and enhance overall crop productivity and sustainability [16].

13.2.2.1 Crop Health Sensors

By deploying IoT-enabled crop health sensors, farmers can continuously collect data on various aspects of crop health, including stress levels, nutrient deficiencies, and pest infestations. These sensors capture information using advanced technologies such as spectral imaging and infrared sensors, allowing for the detection of subtle changes in crop conditions that may indicate potential issues. The collected data is diffused wirelessly to a centralized system, which can be analyzed and processed simultaneously. By accessing this data remotely, farmers can make timely decisions regarding pest control measures, nutrient application, and irrigation adjustments, preventing crop losses and promoting optimal crop growth [17]. IoT-based crop health sensors empower farmers with actionable insights, enabling them to proactively address crop health issues, enhance productivity, and implement sustainable farming practices.

13.2.2.2 Nutrient Level Sensors

IoT plays a crucial role in supporting crop monitoring through nutrient level sensors, enabling farmers to regulate and manage the nutrient status of their plants in real-time. With IoT-enabled nutrient level sensors, farmers can continuously measure and track the levels of essential nutrients such as nitrogen, phosphorus, and potassium in the soil or plant tissues. These sensors provide accurate and timely data wirelessly transmitted to a centralized system for analysis [18]. By accessing this information remotely, farmers can make informed decisions regarding nutrient application, optimizing fertilizer usage, and minimizing nutrient imbalances. IoT-based nutrient level sensors help farmers monitor crop nutrient uptake, detect deficiencies or excesses, and adjust fertilizer regimes accordingly. This targeted approach ensures that crops receive the right amount and balance of nutrients, promoting healthy growth, maximizing yield, and reducing environmental impact [19]. IoT-enabled nutrient level sensors provide farmers with valuable insights for precision nutrient management, facilitating sustainable farming practices and improving overall crop performance.

13.2.2.3 Weather Sensors

IoT is pivotal in supporting crop monitoring through weather sensors, enabling farmers to obtain real-time and accurate weather data for effective crop management. IoT-enabled weather sensors are deployed in the fields to collect data on various

weather parameters such as wind speed, rainfall, temperature, humidity, and solar radiation. By accessing this data remotely, farmers can make decisions varieties regarding irrigation scheduling, pest and disease management, and crop protection measures [20]. In addition, weather sensors provide valuable insights into local weather conditions, enabling farmers to anticipate and respond to potential risks such as frost, heat waves, or heavy rainfall. By integrating weather data with crop growth models and predictive analytics, IoT-enabled weather sensors assist farmers in optimizing planting schedules, adjusting irrigation practices, and implementing timely interventions to mitigate weather-related risks [21].

13.2.3 Livestock Monitoring

Within smart agriculture and IoT, Livestock monitoring refers to continuously tracking and managing livestock using connected sensors and technologies. IoT-enabled devices such as global positioning system (GPS) trackers, health monitoring sensors, and behavior monitoring systems are deployed to collect data on livestock's location, health, and behavior. This data is diffused wirelessly to a primary system for analysis, enabling farmers to remotely monitor and assess the well-being of their livestock, identify signs of illness or distress, optimize feeding schedules, and ensure proper animal welfare and management practices [22].

13.2.3.1 Animal Tracking Devices

IoT-enabled animal tracking devices, such as GPS trackers or RFID tags, are attached to the animals, allowing for real-time tracking and monitoring of their whereabouts. The devices collect and transmit location data wirelessly to a centralized system, which farmers can access remotely. This information enables farmers to monitor grazing patterns, prevent livestock theft or straying, optimize pasture utilization, and enhance overall herd management. Additionally, animal tracking devices facilitate timely intervention in emergencies or incidents, such as illness, calving, or birthing, allowing farmers to provide prompt care and support [23]. IoT-based animal tracking devices provide farmers with valuable insights into the behavior and movement of their livestock, promoting better management practices, ensuring animal welfare, and enhancing operational efficiency in livestock farming.

13.2.3.2 Health Monitoring Sensors

IoT-enabled health monitoring sensors are deployed to collect real-time data on livestock's vital signs, behavior patterns, and other health-related parameters. These sensors may include wearable devices or implanted sensors that measure parameters such as body temperature, heart rate, rumination, and activity levels [23]. The collected data is transmitted wirelessly to a centralized system, where it can be

analyzed and processed. By accessing this information remotely, farmers can identify signs of illness or distress in their animals, enabling them to intervene promptly and provide appropriate medical care. IoT-based health monitoring sensors help farmers detect early symptoms of diseases, monitor recovery progress, and optimize feeding and medication regimes, ultimately ensuring the overall health and well-being of the livestock. This proactive approach to livestock health management enhances animal welfare, reduces mortality rates, and improves farm productivity and profitability [24].

13.2.3.3 Feed Monitoring Systems

IoT-enabled feed monitoring systems utilize sensors and data collection devices to track feed consumption and monitor feeding patterns in real-time. These systems can measure feed intake, duration, and refusals. The collected data is wirelessly transmitted to a centralized platform, allowing farmers to access and analyze the information remotely. By leveraging this data, farmers can accurately assess the feed requirements of their livestock, ensure proper nutrition, and prevent over or underfeeding [25]. IoT-based feed monitoring systems also enable farmers to identify any changes in feeding behavior or irregularities, which may indicate health issues or feeding inefficiencies. This proactive approach to feed management enhances animal nutrition, reduces feed wastage, and improves feed efficiency, ultimately contributing to the livestock operation's overall health, productivity, and profitability [26].

13.3 Data Collection and Data Analysis

Data analysis and collection techniques as supported by IoTs in smart agricultural practices, including data-gathering techniques, analytics and processing, predictive analytics, and decision support systems.

13.3.1 Data-Gathering Techniques

In smart agriculture, data gathering refers to systematically collecting agricultural data using various technologies and sensors. These sensors can monitor parameters, for instance, livestock behavior, soil moisture, nutrient levels, weather conditions, and crop health. The collected data is transmitted wirelessly to a central system for analysis and decision-making. This data-gathering process allows farmers to obtain real-time and accurate information about their crops, soil, and livestock, enabling them to make decisions regarding fertilization, pest control, irrigation, and animal health management [27]. By gathering and analyzing data, farmers can optimize their agricultural practices, improve resource efficiency, increase productivity, and implement sustainable farming techniques.

13.3.1.1 Wireless Sensor Networks

Wireless sensor networks (WSNs) consist of small, interconnected sensors strategically placed throughout the agricultural field to collect and transmit data wirelessly. These sensors can monitor various parameters such as soil moisture, temperature, humidity, light intensity, and air quality. By deploying WSNs, farmers can obtain real-time and accurate information about the conditions of their crops and the environment, as Figure 13.4 illustrates. The sensors in the network communicate with each other and diffuse the collected aggregated information to a central system or cloud platform, where it can be analyzed and utilized for decision-making. This enables farmers to make informed choices regarding irrigation scheduling, fertilization, pest management, and other farming practices. WSNs eliminate the need for manual data collection, reduce labor costs, and provide continuous monitoring capabilities [28]. Using WSNs as a data-gathering technique, smart agriculture optimizes resource allocation, enhances crop productivity, and promotes sustainable and efficient farming practices.

13.3.1.2 Remote Sensing Technologies

These technologies utilize satellite or airborne sensors to capture detailed information about agricultural fields from a distance. Remote sensing provides valuable data on various parameters such as crop health, vegetation indices, soil moisture, temperature, and land cover. By analyzing the imagery and data obtained through remote sensing, farmers can gain insights into crop conditions and identify areas of concern. Remote sensing enables large-scale and continuous monitoring of agricultural areas, allowing farmers to detect early signs of stress, disease outbreaks, or nutrient

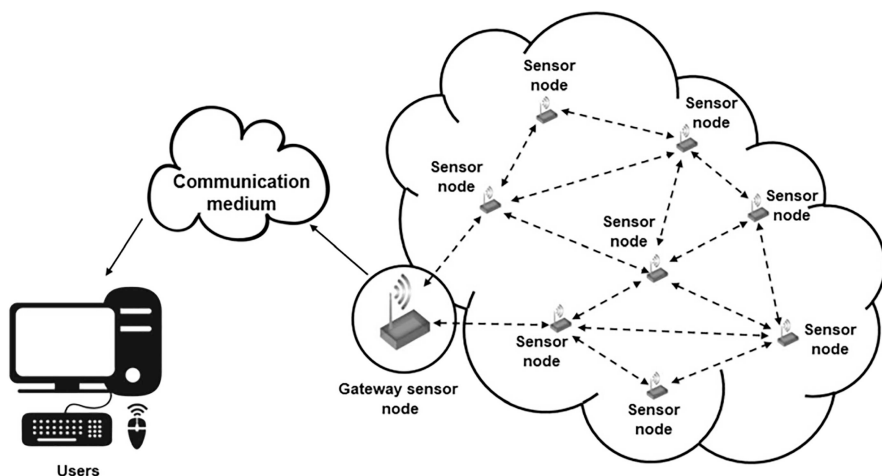


Figure 13.4 Wireless sensor networks application.

deficiencies. This data-driven approach helps optimize resource allocation, improve crop yields, and promote sustainable agricultural practices [29]. Furthermore, remote sensing technologies provide a cost-effective and efficient means of data gathering, enabling farmers to make timely and data-driven decisions for enhanced productivity and profitability in smart agriculture.

13.3.2 Data Analytics and Processing

Data analytics and processing refer to the systematic examination, interpretation, and transformation of raw data into meaningful insights and actionable information through various computational and analytical techniques. This section presents two computational techniques, including cloud and edge computing.

13.3.2.1 Cloud Computing

Through cloud-based platforms and services, agricultural data from various sources such as sensors, drones, or satellite imagery can be securely stored, processed, and analyzed in real-time. Cloud computing offers the scalability, computational power, and storage capabilities required to handle large volumes of agricultural data efficiently. This allows farmers and agricultural stakeholders to leverage advanced analytics techniques, such as machine learning and predictive modeling, to derive valuable insights from the data [30]. Cloud-based data analytics enable farmers to make data-driven crop management, resource allocation, and risk assessment decisions. Furthermore, cloud computing provides seamless collaboration and data sharing among stakeholders, enabling the exchange of information and knowledge to foster innovation and improve agricultural practices [31]. By leveraging cloud computing for data analytics and processing, smart agriculture can unlock the full potential of agricultural data and drive sustainable and efficient farming practices.

13.3.2.2 Edge Computing

In the context of agriculture, edge computing brings computational power and analytics capabilities directly to the field, reducing latency and improving real-time decision-making. With edge computing, data collected from various sensors and devices, such as weather stations or livestock monitors, can be processed and analyzed locally without relying solely on cloud-based solutions. This allows for faster response times and reduced reliance on constant internet connectivity [32]. As a result, edge computing empowers farmers to perform on-site data analytics and gain immediate insights into crop conditions, livestock health, or environmental factors. It also helps in optimizing resource allocation, enabling timely interventions, and improving operational efficiency.

13.3.3 Predictive Analytics and Decision Support Systems

Predictive analytics involves using historical and real-time data to forecast future outcomes or trends, enabling organizations to make informed decisions.

13.3.3.1 Machine Learning Algorithms

Such algorithms can analyze large volumes of agricultural data, including crop sensor data, weather data, and historical yield information, to identify patterns, correlations, and trends. By training on this data, machine learning models can accurately predict various agricultural outcomes, such as crop yield, disease outbreaks, or optimal irrigation schedules [33]. This predictive capability enables farmers to anticipate potential issues, optimize resource allocation, and make informed decisions for improved crop management. Machine learning algorithms also contribute to decision support systems by providing valuable insights and recommendations based on data analysis. As a result, these systems assist farmers in decision-making about planting, pest control, and related farming practices, ultimately enhancing productivity, resource efficiency, and sustainability in smart agriculture [34].

13.3.3.2 Artificial Intelligence Applications

AI algorithms and techniques, such as machine learning, deep learning, and computer vision, can process and analyze vast amounts of agricultural data to extract valuable insights. By leveraging AI, predictive models can be developed to forecast crop yields, identify disease outbreaks, or optimize resource allocation [35]. AI applications can also automate data collection, monitoring, and analysis processes, reducing manual efforts and improving overall efficiency. With AI-driven predictive analytics and decision support systems, smart agriculture can enhance productivity, reduce costs, and foster sustainable farming practices by leveraging the power of artificial intelligence [36].

13.4 Automation and Control Systems

This section presents some selected automation and control systems used in smart agricultural practices like smart irrigation, precision farming, and livestock management.

13.4.1 Smart Irrigation

Smart irrigation refers to the intelligent and automated management of water resources in agricultural or landscaping settings using advanced technologies and systems. It involves the integration of sensors, data analytics, and control mechanisms to optimize irrigation practices based on real-time environmental

conditions and plant water requirements. Smart irrigation systems monitor soil moisture, weather conditions, evapotranspiration rates, and plant health to determine the appropriate timing and amount of water needed for irrigation [37].

13.4.1.1 Automated Irrigation Systems

These systems utilize sensors, controllers, and actuators to automate the irrigation process based on real-time data and predefined parameters. Automated irrigation systems ensure precise and efficient crop delivery by continuously monitoring weather conditions and plant water requirements. For example, the sensors measure soil moisture levels, providing feedback to the controller, which then triggers the irrigation system to supply water only when necessary [38]. This helps prevent overwatering or underwatering, optimize water usage, and promote healthy plant growth. In addition, automated irrigation systems can be programmed to adjust irrigation schedules and durations based on specific crop needs, environmental conditions, and water availability. As a result, farmers can conserve water, reduce costs, improve crop yield, and promote sustainable agricultural practices by implementing smart irrigation systems [39].

13.4.1.2 Water Management and Optimization

By leveraging advanced technologies, data analytics, and real-time monitoring, smart irrigation systems enable farmers to efficiently manage and optimize their water usage in agricultural operations. These systems utilize sensors to measure soil moisture levels, weather conditions, and plant water requirements, allowing for precise and targeted irrigation. Smart irrigation minimizes water wastage, prevents overwatering or underwatering, and promotes optimal plant growth and yield by providing an accurate amount of water at an accurate time. Smart irrigation systems can also be integrated with weather forecasts and historical data to anticipate future water requirements and adjust irrigation schedules accordingly [39]. This proactive approach to water management ensures the conservation of water resources, reduces costs, and promotes sustainable agricultural practices that align with the principles of efficient resource utilization in smart agriculture.

13.4.2 Precision Farming

This subsection presents some selected precision farming approaches that contribute to smart farming.

13.4.2.1 Variable Rate Technologies

Variable rate technologies (VRT) enable farmers to apply inputs, like fertilizers, pesticides, or irrigation, at variable rates across a field based on specific crop

requirements and spatial variability. By utilizing advanced technologies, including GPS, sensors, and mapping software, VRT systems create prescription maps that guide the precise application of inputs. These systems consider factors such as soil fertility, crop growth stage, and historical yield data to determine inputs' optimal rate and placement in different field areas [40]. This targeted approach ensures that resources are utilized efficiently, reducing input wastage, increasing crop productivity, and minimizing environmental impact. VRT enables farmers to address site-specific challenges and optimize input applications to maximize yields while minimizing costs, ultimately leading to improved profitability and sustainable farming practices in precision farming [41].

13.4.2.2 Autonomous Farming Equipment

These advanced machines, such as autonomous tractors, harvesters, and drones, are equipped with sophisticated sensors, GPS technology, and artificial intelligence algorithms that enable them to operate with minimal human intervention. Autonomous farming equipment can perform precise and repeatable tasks, such as planting, spraying, and harvesting, with high accuracy and efficiency. By leveraging real-time data and advanced mapping systems, these autonomous machines can navigate fields, detect crop health issues, and make precise decisions for targeted operations [42]. This level of precision and automation results in optimized resource utilization, reduced labor costs, and increased productivity. Autonomous farming equipment enables farmers to adopt site-specific approaches, such as variable rate application and selective harvesting, to maximize yields, minimize waste, and improve overall farm management. Furthermore, autonomous equipment contributes to sustainable farming practices by reducing chemical usage, improving soil health, and promoting efficient resource allocation in precision farming [43].

13.4.3 Livestock Management

Livestock management refers to overseeing and caring for domesticated animals, such as cattle, sheep, goats, pigs, or poultry, to ensure their well-being, health, and productivity. It involves various activities, including feeding, watering, sheltering, breeding, disease prevention, veterinary care, and record-keeping [44]. Effective livestock management optimizes animal health, growth, and reproduction while maintaining proper nutrition and providing a suitable animal environment.

13.4.3.1 Automated Feeding Systems

These systems utilize advanced technologies and sensors to automate the feeding process for domesticated animals, such as cattle, pigs, or poultry. By leveraging data analysis and real-time monitoring, automated feeding systems can precisely deliver feed to individual animals based on their nutritional needs and growth stages. The

systems can be programmed to distribute the appropriate amount and type of feed, ensuring optimal nutrition and minimizing wastage. Additionally, automated feeding systems can record and analyze feeding patterns, allowing farmers to monitor and manage the health and productivity of their livestock. These systems also contribute to labor efficiency by reducing manual feeding tasks and enabling continuous feeding schedules [45]. By implementing automated feeding systems, farmers can improve feed efficiency, enhance animal health, and optimize production in livestock management, leading to increased profitability and sustainable farming practices.

13.4.3.2 Climate Control and Monitoring

Climate control and monitoring systems are vital in smart agriculture, particularly livestock management. These systems utilize sensors, actuators, and automation technologies to create and maintain optimal climatic conditions within livestock facilities. By monitoring parameters such as temperature, humidity, air quality, and ventilation, climate control systems can adjust and regulate environmental conditions to ensure the animals' comfort, health, and productivity. The systems can automatically control heating, cooling, ventilation, and air circulation to maintain a stable and favorable climate for the livestock [46]. This helps prevent heat stress, minimize disease outbreaks, and reduce mortality rates. Climate control and monitoring systems also enable farmers to track and analyze environmental data, allowing for data-driven decision-making and proactive management.

13.5 Connectivity and Communication

Smart agriculture entails several connectivity and communication; within this section, some standard technologies are demonstrated, including wireless communication technologies and data security and privacy considerations.

13.5.1 Wireless Communication Technologies

Wireless communication technologies transmit information or data between devices or systems without physical cables or wired connections. Instead, these technologies utilize electromagnetic waves to enable wireless communication over varying distances. Wireless communication technologies examples include Radio Frequency Identification (RFID), Bluetooth, Wi-Fi, generational cellular networks (2G, 3G, 4G, 5G and beyond), and Zigbee [47]. These technologies allow for seamless and efficient data transfer, voice communication, and connectivity between devices, enabling the exchange of information and facilitating communication in diverse applications and industries, including telecommunications, IoT, mobile computing, and smart devices. As a result, wireless communication

technologies have significantly transformed how people communicate, collaborate, and access information, providing flexibility, mobility, and connectivity in various aspects of daily life and technological advancements [48].

13.5.1.1 Wi-Fi

It enables the connectivity of various devices and sensors in agricultural operations, facilitating data transfer and communication in real-time. Wi-Fi networks provide a reliable and high-speed connection, allowing agriculturalists to remotely control and monitor different aspects of their farming operations. With Wi-Fi, sensors can collect and transmit data on parameters like temperature, soil moisture, and crop health, providing farmers with valuable insights for decision-making [49]. Wi-Fi connectivity also supports integrating smart devices and systems, enabling seamless communication and coordination. As a result, farmers can access and analyze data from multiple sources, like weather forecasts or market trends, to optimize farming practices and improve productivity. Moreover, Wi-Fi connectivity in smart agriculture enables the management and control of automated systems, such as irrigation or precision farming equipment, allowing for efficient resource utilization and sustainable farming practices [50].

13.5.1.2 Cellular Networks (5G and Beyond)

Cellular networks, specifically 5G and beyond, offer significant benefits in the context of smart agriculture. These wireless communication technologies provide fast, reliable, and widespread connectivity, enabling seamless data transfer and communication across agricultural operations. With the high bandwidth and low latency of 5G, farmers can access real-time information and make timely decisions for improved efficiency and productivity [51]. Cellular networks support the connectivity of various devices and sensors in smart agriculture, allowing for remote monitoring and control of equipment, environmental conditions, and livestock health. The enhanced capacity and coverage of 5G networks enable the deployment of advanced technologies, such as drones and autonomous vehicles, for precision farming tasks. These networks also facilitate the integration of emerging technologies like AI and edge computing, enabling more sophisticated data analysis and decision-making capabilities [52]. With the continued development of cellular networks, including upcoming 6G technologies, smart agriculture will benefit from even faster and more reliable wireless communication, unlocking the further potential for automation, optimization, and sustainable farming practices.

13.5.1.3 LPWAN (Low-Power Wide-Area Networks)

LPWANs offer long-range connectivity with low power consumption, making them ideal for applications that require low data rates and long battery life. In

smart agriculture, LPWAN enables the deployment of a wide range of low-power devices and sensors across large agricultural areas [53]. By leveraging LPWAN, farmers can collect and transmit data from remote locations, enabling real-time monitoring and analysis. In addition, LPWAN networks provide cost-effective and efficient connectivity, allowing farmers to extend their monitoring capabilities and make data-driven decisions. With LPWAN, smart agriculture systems can operate in challenging environments with limited power and infrastructure, providing a scalable and sustainable solution for precision agriculture.

13.5.2 Data Security and Privacy Considerations

Security and privacy are often concerns that arise when it comes to the application of smart applications; we consider two approaches to this.

13.5.2.1 Encryption and Authentication

Encryption converts data into a coded form that authorized parties can only access and understand. By encrypting data, smart agriculture systems can protect information from unauthorized access or interception, safeguarding it from potential threats or breaches [54]. On the other hand, authentication verifies the identity of users or devices accessing the system, ensuring that only authorized entities can access and interact with the data. This helps in preventing unauthorized tampering, manipulation, or misuse of data. Encryption and authentication mechanisms are vital for maintaining the integrity and confidentiality of sensitive agricultural data, including crop information, livestock records, and farm management details [55]. Smart agriculture systems can instill trust, foster data-sharing collaborations, and ensure compliance with privacy regulations by prioritizing data security and privacy considerations through encryption and authentication.

13.5.2.2 Data Ownership and Access Control

Data ownership and access control are essential to smart agriculture's data security and privacy considerations. In the context of smart agriculture systems, various stakeholders, including farmers, agricultural service providers, and technology vendors, collect and analyze valuable agricultural data. Data ownership refers to the rights and control over the data generated or collected during farming operations. Clear data ownership ensures farmers retain control and decision-making authority over their data, preventing unauthorized use or exploitation [56]. Access control mechanisms, on the other hand, govern who can access, modify, or share the data. By implementing robust access control protocols, smart agriculture systems can ensure that only authorized individuals or entities can access specific data sets, maintaining confidentiality and preventing unauthorized data breaches. Effective data ownership and access control mechanisms enable farmers to protect their data

assets, maintain their privacy, and make informed decisions about data sharing and utilization, to foster trust and accountability in the smart agriculture ecosystem [57].

13.6 Selected Case Studies

As explained below, examples of successful IoT implementations in smart agriculture range from soil analysis to farm management.

13.6.1 Smart Irrigation System with IoT Sensors

One successful implementation of IoT in smart agriculture is using smart irrigation systems with IoT sensors. Farmers can deploy soil moisture sensors connected to an IoT network in their fields. These sensors continuously monitor soil moisture levels and transmit real-time data to a central control system. The control system, equipped with IoT technology, analyzes the data and triggers automated irrigation based on specific thresholds and crop water requirements [58]. For example, if the soil moisture drops below a certain level, the system automatically activates the irrigation system to provide the required amount of water to the crops. This implementation helps optimize water usage, reduce water waste, and ensure crops receive the precise irrigation they need for healthy growth.

13.6.2 Livestock Monitoring with Wearable IoT Devices

Another successful IoT implementation in smart agriculture is wearable IoT devices for livestock monitoring. Farmers can attach IoT-enabled devices, such as GPS trackers or health monitoring sensors, to individual animals. These devices collect data on the animals' location, behavior, health parameters, and other vital information. The data is transmitted wirelessly to a central database or cloud-based platform, where it is processed and analyzed in real-time. Farmers can then remotely monitor the health and behavior of their livestock, detect any anomalies or signs of distress, and take prompt action [59]. For instance, if a cow's activity level or body temperature deviates from the normal range, an alert can be sent to the farmer, enabling them to intervene and provide appropriate care. This IoT implementation enhances animal welfare, enables early detection of diseases or injuries, and improves overall livestock management practices [60].

13.6.3 Crop Monitoring and Pest Management with IoT and AI

Crop monitoring and pest management are critical aspects of smart agriculture, and IoT combined with AI has proven to be a successful implementation in this area. Farmers can deploy a network of IoT sensors and cameras in their fields to

monitor various parameters such as temperature, humidity, soil conditions, and plant growth. These sensors collect data and transmit it to an AI-powered analytics platform that analyzes it and provides valuable insights. By leveraging machine learning algorithms, the system can detect patterns, identify potential pest infestations or diseases, and predict crop growth and yield. This information enables farmers to take proactive measures such as targeted pesticide application or adjusting irrigation schedules to mitigate risks and optimize crop health [61]. For example, if the analytics platform detects abnormal temperature and humidity levels combined with specific leaf patterns, it can alert the farmer about a potential pest outbreak and recommend suitable pest control strategies. This implementation helps farmers make data-driven decisions, improve crop yield, reduce chemical usage, and enhance overall crop management practices [62].

13.6.4 Smart Greenhouses with IoT Automation

Smart greenhouses are another successful application of IoT in smart agriculture. IoT technology can be integrated into greenhouse systems to control and monitor environmental conditions like Humidity, Temperature, Light, and Carbon dioxide levels. IoT sensors throughout the greenhouse collect data and transmit it to a centralized control system. The control system, powered by IoT, analyzes the data and automatically adjusts parameters to maintain ideal plant growth conditions [63]. For instance, if the temperature inside the greenhouse exceeds a set threshold, the IoT-controlled system can activate cooling mechanisms such as ventilation or shade systems to decrease the temperature. If the humidity drops below a certain level, the system can trigger misting systems to increase humidity. This automation helps optimize plant growth, minimize energy consumption, and ensure the efficient use of resources. Farmers can also remotely monitor and control the greenhouse environment through a mobile app or web interface, providing flexibility and convenience in managing their crops [64].

Farmers and agricultural enterprises can reap numerous benefits from implementing IoT in smart agriculture. IoT technologies enable farmers to make data-driven decisions, optimizing resource allocation and boosting productivity. For example, farmers can implement precise irrigation and fertilization strategies by monitoring and analyzing soil moisture, temperature, and crop health data, leading to healthier and more abundant crop yields. Moreover, IoT-based systems facilitate efficient resource management, minimizing waste and maximizing resource utilization [65]. Real-time monitoring of parameters such as soil moisture, weather conditions, and crop requirements allows farmers to apply irrigation and fertilizers only when necessary, reducing waste and minimizing environmental impact. This leads to cost savings and promotes sustainable farming practices, improving environmental stewardship and ensuring long-term sustainability.

IoT in smart agriculture enhances decision-making capabilities. Real-time data collection and analysis provide farmers with accurate and up-to-date information

on crop conditions, weather patterns, and market trends. This empowers them to make informed decisions promptly, adjust their strategies, mitigate risks, and capitalize on market opportunities. Additionally, IoT-enabled systems offer remote monitoring and control, enabling farmers to manage their operations from anywhere [66]. They can access data on soil conditions, livestock health, or greenhouse environments, facilitating remote management and saving time and effort. Furthermore, early detection of pests, diseases, or irregularities in crop growth through IoT sensors and data analytics allows farmers to take proactive measures. This includes targeted pest control or adjustments in irrigation schedules, preventing potential crop losses, and ensuring better plant health.

Therefore, IoT in smart agriculture provides farmers and agricultural enterprises with valuable insights, improved efficiency, and sustainable practices. It enhances productivity, resource management, decision-making, and remote monitoring capabilities [67]. The early detection of issues and implementation of preventive measures further contribute to increased profitability and resilience in the agricultural sector. The following section depicts some challenges and the future trends of agricultural IoT.

13.7 Future Trends and Challenges

Future trends of Agricultural IoTs involve integrating emerging technologies, edge computing, sustainability practices, data interoperability, and addressing challenges related to data privacy, security, and accessibility. Overcoming these challenges will pave the way for the widespread adoption of IoT technologies in smart agriculture, transforming the industry and enabling more efficient, sustainable, and productive farming practices.

13.7.1 Integration with Emerging Technologies

Agricultural IoTs' future lies in integrating emerging technologies like AI, blockchain, ML, AI, and ML algorithms that can leverage the vast amount of data IoT sensors collect to provide more accurate predictions, optimize resource management, and automate decision-making processes. Likewise, blockchain technology can enhance data security, traceability, and transparency in agricultural supply chains, ensuring the integrity of data and transactions [68].

13.7.2 Edge Computing and Edge Analytics

As the volume of data generated by IoT sensors increases, there is a need for real-time processing and analysis at the network's edge. Edge computing enables faster response times, reduced latency, and efficient use of network bandwidth [69]. In addition, edge analytics allows for data processing and insights generation closer to the data source, enhancing scalability and reducing reliance on cloud infrastructure.

13.7.3 Sustainable and Regenerative Practices

The future of smart agriculture will focus on sustainable and regenerative practices. IoT technologies can aid in optimizing resource usage, reducing environmental impact, and promoting sustainable farming techniques such as precision farming, organic farming, and integrated pest management. Furthermore, integrating IoT with environmental sensors can facilitate real-time monitoring of soil health, water quality, and air quality, enabling farmers to make informed decisions prioritizing sustainability [70].

13.7.4 Data Interoperability and Standardization

The interoperability and standardization of data across different IoT platforms and devices remain challenging. To fully unlock the potential of Agricultural IoTs, there is a need for common data standards and protocols that enable seamless integration and data exchange between different systems and stakeholders [71]. This will facilitate data sharing, collaboration, and the development of comprehensive analytics solutions.

13.7.5 Data Privacy and Security

The increasing reliance on data collection and sharing makes ensuring data privacy and security crucial. Agricultural IoT systems must implement robust data encryption, access controls, and authentication mechanisms to protect sensitive information. In addition, adhering to privacy regulations and best practices will be essential to maintain trust among farmers, consumers, and other stakeholders [72].

13.7.6 Digital Divide and Accessibility

Bridging the digital divide and ensuring accessibility to IoT technologies is challenging, particularly for small-scale farmers in remote areas or developing nations [73]. Efforts should be made to provide affordable and user-friendly IoT solutions, promote digital literacy [74], and address infrastructure gaps to ensure equitable access to the benefits of Agricultural IoTs in protecting plants in autonomous disease detection and classification [75].

13.8 Lessons Learnt and Conclusion

The implementation of IoT in smart agriculture highlights the importance of leveraging data for informed decision-making. Farmers can optimize resource allocation, mitigate risks, and improve farm productivity by collecting and analyzing real-time data from sensors and devices. The successful implementation

of IoT in smart agriculture often involves the integration of various technologies such as AI, ML, and cloud computing. Combining these technologies allows for advanced data analytics, automation, and remote monitoring, enabling farmers to make more accurate and timely decisions.

Sustainability and resource optimization: IoT in smart agriculture promotes sustainable farming practices by optimizing resource management. Precise irrigation, targeted fertilization, and efficient energy usage contribute to environmental conservation and the long-term sustainability of agricultural operations. The adoption of IoT in smart agriculture requires collaboration and knowledge sharing among farmers, researchers, and technology providers. Sharing best practices, case studies, and lessons learned can accelerate the adoption and implementation of IoT technologies in the agricultural sector.

The integration of IoT in smart agriculture holds great promise for the future of farming. Farmers can optimize crop production, reduce resource waste, and improve overall farm management practices through IoT sensors, devices, and data analytics. The benefits of IoT in smart agriculture include increased productivity, efficient resource management, sustainability, and improved decision-making capabilities. However, the successful implementation of IoT in smart agriculture also faces challenges such as data security, interoperability, and accessibility. Addressing these challenges requires collaborative efforts from stakeholders, including policymakers, technology providers, and farmers. As we progress, we must continue investing in research and development, promote knowledge exchange, and support farmers to adopt and utilize IoT technologies effectively. By embracing IoT in smart agriculture and overcoming the associated challenges, we can pave the way for a more efficient, sustainable, and productive future in the agricultural industry.

References

1. Y. B. Bakare, "Machine Learning-Based Smart Irrigation System and Soil Nutrients Analysis to Increase Productivity in Agriculture Field," *AIP Conference Proceedings*, vol. 2523, no. 1, 2023. 10.1063/5.0116007.
2. M. Arya, and G. Hanumat Sastry, "Effective LSTM Neural Network with Adam Optimizer for Improving Frost Prediction in Agriculture Data Stream," in *International Conference on Modelling and Development of Intelligent Systems*, Cham: Springer Nature Switzerland, pp. 3–17, 2022. 10.1007/978-3-031-27034-5_1.
3. A. K. Gupta, N. R. N. V. G. Rao, P. Bilgaiyan, N. K. Shruthi, and R. Shanmugam, "Role of Artificial Intelligence in Agriculture—A Paradigm Shift," in *International Conference on Cyber Security, Privacy and Networking*, Cham: Springer International Publishing, pp. 356–360, 2021. 10.1007/978-3-031-22018-0_33.
4. J. Balduque-Gil et al., "Big Data and Machine Learning to Improve European Grapevine Moth (*Lobesia botrana*) Predictions," *Plants*, vol. 12, no. 3, 2023. 10.3390/plants12030633.

5. P. Das, M. Singh, D. A. Karras, and D. G. Roy, "Block-A-City: An Agricultural Application Framework Using Blockchain for Next-Generation Smart Cities," *IETE Journal of Research*, pp. 1–11, 2023. 10.1080/03772063.2022.2162982.
6. K. Kalinaki, W. Shafik, T. J. Gutu, and O. A. Malik, "Computer Vision and Machine Learning for Smart Farming and Agriculture Practices," in *Artificial Intelligence Tools and Technologies for Smart Farming and Agriculture Practices*, IGI Global, pp. 79–100, 2023. 10.4018/978-1-6684-8516-3.ch005.
7. C. Yu, L. Li, J. Li, P. Qin, and B. Zhang, "The Evaluation of Enterprise Supply Chain Intelligent Manufacturing System for Agricultural Interconnection Data Based on Machine Learning," *Expert Systems*, 2023. 10.1111/exsy.13259.
8. O. Jouini, and K. Sethom, "AgriBloT: A Blockchain-Based IoT Architecture for Crop Insurance," in *Lecture Notes in Networks and Systems*, Cham: Springer International Publishing, pp. 340–350, 2023. 10.1007/978-3-031-28694-0-32.
9. W. S. Kim, W. S. Lee, and Y. J. Kim, "A Review of the Applications of the Internet of Things (IoT) for Agricultural Automation," *Journal of Biosystems Engineering*, 45, pp. 385–400, 2020. 10.1007/s42853-020-00078-3.
10. W. Shafik, and A. Tufail, "Energy Optimization Analysis on Internet of Things," in *Advanced Technology for Smart Environment and Energy*, Cham: Springer International Publishing, pp. 1–16, 2023. 10.1007/978-3-031-25662-2_1.
11. W. Shafik, "Making Cities Smarter: IoT and SDN Applications, Challenges, and Future Trends," in *Opportunities and Challenges of Industrial IoT in 5G and 6G Networks*, IGI Global, pp. 73–94, 2023. 10.4018/978-1-7998-9266-3.ch004.
12. A. G. Menon, and M. Prabhakar, "Intelligent IoT-Based Monitoring Rover for Smart Agriculture Farming in Rural Areas," in *Lecture Notes in Networks and Systems*, 2023. 10.1007/978-981-19-0098-3_60.
13. V. Parkhi, N. Chavhan, S. Chandak, B. Chaware, and P. Bongarde, "An IoT Based Environment Monitoring & Controlling System for Food Grain Warehouse," in *Lecture Notes in Networks and Systems*, 2023. 10.1007/978-981-19-5845-8_16.
14. S. Bera, T. Dey, A. Mukherjee, and R. Buyya, "E-CropReco: A Dew-Edge-Based Multi-parametric Crop Recommendation Framework for Internet of Agricultural Things," *Journal of Supercomputing*, 2023. 10.1007/s11227-023-05131-4.
15. S. Watanabe, Y. Terashima, and R. Kiyohara, "Effects Detection with Plant Growth in the Sensor Network," in *IEEE International Conference on Consumer Electronics*, 2023. 10.1109/ICCE56470.2023.10043522.
16. P. Navya, and D. Sudha, "Artificial Intelligence-based Robot for Harvesting, Pesticide Spraying and Maintaining Water Management System in Agriculture Using IoT," *AIP Conference Proceedings*, 2023. 10.1063/5.0110258.
17. K. Chatterjee, A. Singh, and Neha, "A Blockchain-Enabled Security Framework for Smart Agriculture," *Computers and Electrical Engineering*, vol. 106, 2023. 10.1016/j.compeleceng.2023.108594.
18. J. B. Prajapati, R. Barad, M. B. Patel, K. Saini, D. Prajapati, and P. Engineer, "Smart Farming Ingredients: IoT Sensors, Software, Connectivity, Data Analytics, Robots, Drones, GIS-GPS," in *Applying Drone Technologies and Robotics for Agricultural Sustainability*, 2023. 10.4018/978-1-6684-6413-7.ch003.
19. W. Shafik, S. M. Matinkhah, and M. Ghasemazade, "Fog-Mobile Edge Performance Evaluation and Analysis on Internet of Things," *Journal of Advance Research in Mobile Computing*, vol. 1, no. 3. 10.5281/zenodo.3591228.

20. W. Shafik, "Cyber Security Perspectives in Public Spaces: Drone Case Study," in *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems 2023*, IGI Global, pp. 79–97. 10.4018/978-1-6684-7207-1.ch004.
21. V. Nehra, M. Sharma, and V. Sharma, "IoT Based Smart Plant Monitoring System," in *2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence) 2023*, pp. 60–65. 10.1109/Confluence56041.2023.10048792.
22. M. Farshid, J. Shiddike, A. Ahmed, I. Karim, and A. K. M. M. Islam, "IoT-Based Agriculture Trend Prediction Based on Weather Data," in *Smart Innovation, Systems and Technologies*, 2023. 10.1007/978-981-19-3571-8_15.
23. A. Khanna, and S. Kaur, "An Empirical Analysis on Adoption of Precision Agricultural Techniques among Farmers of Punjab for Efficient Land Administration," *Land Use Policy*, vol. 126, 2023. 10.1016/j.landusepol.2022.106533.
24. J. Sajid, K. Hayawi, A. W. Malik, Z. Anwar, and Z. Trabelsi, "A Fog Computing Framework for Intrusion Detection of Energy-Based Attacks on UAV-Assisted Smart Farming," *Applied Sciences*, vol. 13, no. 6, p. 3857, 2023. 10.3390/app13063857.
25. G. Peruzzi, A. Pozzebon, and M. Van Der Meer, "Fight Fire with Fire: Detecting Forest Fires with Embedded Machine Learning Models Dealing with Audio and Images on Low Power IoT Devices," *Sensors*, vol. 23, no. 2, 2023. 10.3390/s23020783.
26. S. A. Sofi, and S. Zahoor, "Internet of Things-Enabled Irrigation System in Precision Agriculture," in *Smart Innovation, Systems and Technologies*, pp. 201–211, 2023. 10.1007/978-981-19-7524-0_18.
27. S. K. Kabilish, D. Mohanapriya, P. Suseendhar, J. Indra, T. Gunasekar, and N. Senthilvel, "Research on Artificial Intelligence Based Fruit Disease Identification System (AI-FDIS) with the Internet of Things (IoT)," *Journal of Intelligent & Fuzzy Systems*, pp. 1–6, 2023. 10.3233/jifs-222017.
28. A. J. Simla, R. Chakravarthi, and L. M. Leo, "Agricultural Intrusion Detection (AID) Based on the Internet of Things and Deep Learning with the Enhanced Lightweight M2M Protocol," *Soft Computing*, 2023. 10.1007/s00500-023-07935-1.
29. D. Dutta, C. Mazumder, A. Banerjee, P. Karmakar, D. Mukherjee, and A. Mukherjee, "IoT-Based Smart Monitoring of Soil Parameters for Agricultural Field," in *Lecture Notes in Networks and Systems*, pp. 593–604, 2023. 10.1007/978-981-19-5224-1_60.
30. E. Marín-García, J.-N. Torres-Marín, and A. Chaverra-Lasso, "Smart Greenhouse and Agriculture 4.0," *Revista Científica*, vol. 46, no. 1, pp. 37–50, 2023. 10.14483/23448350.19816.
31. Y. Gamal, A. Soltan, L. A. Said, A. H. Madian, and A. G. Radwan, "Smart Irrigation Systems: Overview," *IEEE Access*, 2023. 10.1109/ACCESS.2023.3251655.
32. C. Amarendra, and T. R. Reddy, "CNN Based Animal Repelling Device for Crop Protection," in *Advances in Transdisciplinary Engineering*, 2023. 10.3233/ATDE221256.
33. M. S. Deelip, and K. Govinda, "ExpSFROA-Based DRN: Exponential Sunflower Rider Optimization Algorithm-Driven Deep Residual Network for the Intrusion Detection in IoT-Based Plant Disease Monitoring," *International Journal of Semantic Computing*, vol. 17, no. 1, pp. 5–13, 2023. 10.1142/S1793351X22400165.
34. A. Laha, B. Saha, A. Banerjee, P. Karmakar, D. Mukherjee, and A. Mukherjee, "IoT-Based Automatic Irrigation Scheduling Using MQTT Protocol," in *Lecture Notes in Networks and Systems*, 2023. 10.1007/978-981-19-5224-1_58.

35. S. Khattar, and T. Verma, "Enhancement of the Performance and Accuracy of Soil Moisture Data Transmission in IOT," in *IOP Conference Series: Earth and Environmental Science*, 2023. 10.1088/1755-1315/1110/1/012001.
36. P. Goliński, P. Sobolewska, B. Stefańska, and B. Golińska, "Virtual Fencing Technology for Cattle Management in the Pasture Feeding System—A Review," *Agriculture (Switzerland)*, vol. 13, no. 1, 2023. 10.3390/agriculture13010091.
37. J. M. Cadenas, M. C. Garrido, and R. Martínez-España, "A Methodology Based on Machine Learning and Soft Computing to Design More Sustainable Agriculture Systems," *Sensors*, vol. 23, no. 6, 2023. 10.3390/s23063038.
38. A. Bholā, S. Srivastava, A. Noonā, B. Sharma, and S. K. Narang, "A Status Quo of Machine Learning Algorithms in Smart Agricultural Systems Employing IoT-Based WSN," in *Machine Intelligence, Big Data Analytics, and IoT in Image Processing*, 2023. 10.1002/9781119865513.ch8.
39. R. Kumar, Harpal, O. Prakash, N. K. Lohiya, and S. Kumar, "IoT Based Smart Irrigation System Using Sensors: A Revolutionary Idea in the Field of Agriculture in India," in *Advances in Transdisciplinary Engineering*, 2023. 10.3233/atde221261.
40. B. Di Martino, L. C. Cante, A. Esposito, and M. Graziano, "Towards a Methodology for the Semantic Representation of Iot Sensors and BPMNs to Discover Business Process Patterns: A Smart Irrigation Case Study," in *Lecture Notes in Networks and Systems*, 2023. 10.1007/978-3-031-20029-8_24.
41. R. Murakami, and H. Yamamoto, "Sensor Network System with Dynamic Service Deployment Depending on Network Condition for Smart Aquaponics," in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2023. 10.1109/ICCE56470.2023.10043392.
42. G. B, "LoRa and IoT Based Smart Irrigation System," *International Journal of Scientific Research in Engineering and Management*, vol. 07, no. 03, 2023. 10.55041/ijserm18124.
43. M. Ehsanifar, F. Dekamini, C. Spulbar, R. Birau, M. Khazaei, and I. C. Bărbăcioru, "A Sustainable Pattern of Waste Management and Energy Efficiency in Smart Homes Using the Internet of Things (IoT)," *Sustainability*, vol. 15, no. 6, 2023. 10.3390/su15065081.
44. M. Saban et al., "A Smart Agricultural System Based on PLC and a Cloud Computing Web Application Using LoRa and LoRaWan," *Sensors*, vol. 23, no. 5, 2023. 10.3390/s23052725.
45. R. Aarthy, D. Sivakumar, and V. Mariappan, "Smart Soil Property Analysis Using IoT: A Case Study Implementation in Backyard Gardening," *Procedia Computer Science*, vol. 218, pp. 2842–2851, 2023. 10.1016/j.procs.2023.01.255.
46. E. Simanungkalit, M. Husna, and J. S. Tarigan, "Smart Farming on IoT-Based Aeroponik Systems," *Sinkron*, vol. 8, no. 1, 2023. 10.33395/sinkron.v8i1.11988.
47. T. Anandhi, P. Malathi, D. Deepa, M. S. Roobini, and G. Nagarajan, "Enhancing Agricultural System and Agro Food Transportation Management Using IoT," in *Lecture Notes in Networks and Systems*, 2023. 10.1007/978-981-19-2538-2_22.
48. B. Prasath, and M. Akila, "IoT-based Pest Detection and Classification Using Deep Features with Enhanced Deep Learning Strategies," *Engineering Applications of Artificial Intelligence*, vol. 121, 2023. 10.1016/j.engappai.2023.105985.

49. S. Yonbawi et al., "Modeling of Sensor Enabled Irrigation Management for Intelligent Agriculture Using Hybrid Deep Belief Network," *Computer Systems Science and Engineering*, vol. 46, no. 2, 2023. 10.32604/csse.2023.036721.
50. L. Lucangeli, E. D'Angelantonio, and A. Pallotti, "Automatic Monitoring IoT System for Phytosanitary Products in Agricultural Machinery," in *Lecture Notes in Electrical Engineering*, 2023. 10.1007/978-3-031-26066-7_41.
51. A. Ikidid, A. El Fazziki, and M. Sadgal, "Internet of Things and Agent-based System to Improve Water Use Efficiency in Collective Irrigation," *Computer Science and Information Systems*, vol. 29, no. 1, 2023. 10.2298/CSIS220227062I.
52. P. Ghutke, and R. Agrawal, "An IoT-based Immersive Approach to Sustainable Farming," in *Irrigation and Drainage - Recent Advances*, 2023. 10.5772/intechopen.105449.
53. A. A. Junior, T. J. A. da Silva, and S. P. Andrade, "Smart IoT lysimetry System by Weighing with Automatic Cloud Data Storage," *Smart Agricultural Technology*, vol. 4, 2023. 10.1016/j.atech.2023.100177.
54. Y. Jun, A. Craig, W. Shafik, and L. Sharif, "Artificial Intelligence Application in Cybersecurity and Cyberdefense," *Wireless Communications and Mobile Computing*, vol. 2021, 2021. 10.1155/2021/3329581.
55. L. Zhao et al., "Artificial Intelligence Analysis in Cyber Domain: A Review," *International Journal of Distributed Sensor Networks*, vol. 18, no. 4, 2022. 10.1177/15501329221084882.
56. X. Y. Ma, J. Tong, F. Jiang, M. Xu, L. M. Sun, and Q. Y. Chen, "Application of Deep Learning to Production Forecasting in Intelligent Agricultural Product Supply Chain," *Computers, Materials and Continua*, vol. 74, no. 3, 2023. 10.32604/cmc.2023.034833.
57. S. Mathi, R. Akshaya, and K. Sreejith, "An Internet of Things-based Efficient Solution for Smart Farming," *Procedia Computer Science*, vol. 218, 2023. 10.1016/j.procs.2023.01.252.
58. A. Mehla, and S. S. Deora, "Use of Machine Learning and IoT in Agriculture," in *EAI/Springer Innovations in Communication and Computing*, 2023. 10.1007/978-3-031-04524-0_16.
59. M. G. Nayagam, B. Vijayalakshmi, K. Somasundaram, M. A. Mukunthan, C. A. Yogaraja, and P. Partheeban, "Control of Pests and Diseases in Plants Using IOT Technology," *Measurement: Sensors*, vol. 26, 2023. 10.1016/j.measen.2023.100713.
60. S. Habib, S. Alyahya, M. Islam, A. M. Alnajim, A. Alabdulatif, and A. Alabdulatif, "Design and Implementation: An IoT-Framework-Based Automated Wastewater Irrigation System," *Electronics (Switzerland)*, vol. 12, no. 1, 2023. 10.3390/electronics12010028.
61. M. Harisudin, Kusnandar, E. W. Riptanti, N. Setyowati, and I. Khomah, "Determinants of the Internet of Things Adoption by Millennial Farmers," *AIMS Agriculture and Food*, vol. 8, no. 2, 2023. 10.3934/agrfood.2023018.
62. N. Tsolakis, T. S. Harrington, and J. S. Strai, "Leveraging Automation and Data-driven Logistics for Sustainable Farming of High-value Crops in Emerging Economies," *Smart Agricultural Technology*, vol. 4, 2023. 10.1016/j.atech.2022.100139.
63. G. Garg, S. Gupta, P. Mishra, A. Vidyarthi, A. Singh, and A. Ali, "CROPCARE: An Intelligent Real-Time Sustainable IoT System for Crop Disease Detection Using Mobile Vision," *IEEE Internet Things Journal*, vol. 10, no. 4, 2023. 10.1109/JIOT.2021.3109019.

64. J. L. Chong, K. W. Chew, A. P. Peter, H. Y. Ting, and P. L. Show, "Internet of Things (IoT)-Based Environmental Monitoring and Control System for Home-Based Mushroom Cultivation," *Biosensors*, vol. 13, no. 1, p. 98, 2023. 10.3390/bios13010098.
65. Z. Yang, L. Jianjun, H. Faqiri, W. Shafik, A. Talal Abdulrahman et al., "Green Internet of Things and Big Data Application in Smart Cities Development," *Complexity*, pp. 1–5, 2021. 10.1155/2021/4922697.
66. R. R. Patil, S. Kumar, R. Rani, P. Agrawal, and S. K. Pippal, "A Bibliometric and Word Cloud Analysis on the Role of the Internet of Things in Agricultural Plant Disease Detection," *Applied System Innovation*, vol. 6, no. 1, 2023. 10.3390/asi6010027.
67. I. Roussaki et al., "Building an Interoperable Space for Smart Agriculture," *Digital Communications and Networks*, vol. 9, no. 1, 2023. 10.1016/j.dcan.2022.02.004.
68. S. Ahmadzadeh, T. Ajmal, R. Ramanathan, and Y. Duan, "A Comprehensive Review on Food Waste Reduction Based on IoT and Big Data Technologies," *Sustainability*, vol. 15, no. 4, 2023. 10.3390/su15043482.
69. S. Bimonte et al., "Data-centric UML Profile for Agroecology Applications: Agricultural Autonomous Robots Monitoring Case Study," *Computer Science and Information Systems*, vol. 29, no. 1, 2023. 10.2298/CSIS220301064B.
70. A. El-Ghamry, A. Darwish, and A. E. Hassanien, "An Optimized CNN-Based Intrusion Detection System for Reducing Risks in Smart Farming," *Internet of Things*, vol. 22, 2023. 10.1016/j.iot.2023.100709.
71. N. N. Thilakarathne, M. S. A. Bakar, P. E. Abas, and H. Yassin, "Towards Making the Fields Talks: A Real-Time Cloud Enabled IoT Crop Management Platform for Smart Agriculture," *Front Plant Science*, vol. 13, 2023. 10.3389/fpls.2022.1030168.
72. A. Vema, J. Sharma, and P. Bhargav, "Analysis on Agriculture Management and Monitoring Using IoT Technology for Security of Workers and to Boost Their Psychology for Nutritional Agricultural Production," *Journal for ReAttach Therapy and Developmental Diversities*, vol. 6, no. 2, pp. 154–158, 2023.
73. W. Shafik, A. Tufail, L. C. De Silva, and R. A. A. H. M. Apong, "Using a Novel Convolutional Neural Network for Plant Pests Detection and Disease Classification," *Journal of the Science of Food and Agriculture*, vol. 103, no. 2, pp. 5849–5861, 2023. 10.1002/jsfa.12700.
74. W. Shafik, A. Tufail, A. Namoun, L. C. De Silva, and R. A. A. H. M. Apong, "A Systematic Literature Review on Plant Disease Detection: Techniques, Dataset Availability, Challenges, Future Trends, and Motivations," *IEEE Access*, pp. 59174–59203, 2023. 10.1109/ACCESS.2023.3284760.
75. S. S. Mohan, R. Venkat, S. Rahaman, M. Vinayak, and B. H. Babu, "Role of AI in Agriculture: Applications, Limitations and Challenges: A Review," *Agricultural Reviews*, vol. 44, no. 2, pp. 231–237, 2023. 10.18805/ag.R-2215.

Chapter 14

Smart IoT-Based Air Quality Monitoring System

S. Devi Mahalakshmi, S. Karkuzhali, and
G. Shenbagalakshmi

Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India

14.1 Introduction

In the modern world, the environment around us gets polluted due to the emission of smoke and other harmful gases. Air Pollution is the biggest problem in most countries. Air pollution in the atmosphere is harmful to the health of living organisms and causes damage to the climate. There are different types of air pollutants, such as gases like Carbon Monoxide, Nitrogen Dioxide, Sulfur dioxide, Ozone, etc., and fine particulate molecules. Harmful gases may cause some health problems like eye infection, asthma, irritation of the throat, and some allergies. It also causes death in some cases. Air pollution is mainly caused by the emission of gases by vehicles and the growing industries.

For the past five years, air pollution in India rises by 15%. Delhi, Lucknow, Patna, and Ahmadabad are the mainly affected states of air pollution and have the highest air quality index due to vehicles and industries. Both human and natural disasters can generate air pollution. Air pollution is mainly caused by the combustion of fossil fuels, emission of gases from industries.

We have designed a system to overcome these difficulties. People can know the concentration of different gases in the air by this system. It also predicts the level of air quality in the future using the past 2 or 3 days record. Industries can also use this system to check the air quality level. This system can also be used in small and large areas. Industries, Homes, and other places can use this system to know the present air quality. It monitors the concentration of air completely and updates the levels of the air.

14.2 Literature Survey

Camprodon et al. represent Smart Citizen, a flexible, easy to use, and fully open solution for environmental monitoring. It is used for particulate matter, Carbon Monoxide, Nitrogen Dioxide, Noise levels, and many other indicators [1]. Huang et al. developed a crowd-source-based sensing system for monitoring fine-grained air quality monitoring in urban environment [2]. Thomas et al. developed a distributed low-cost particular matter sensor for air pollution monitoring [3]. Ennio et al. developed a daily activities recognition system through machine learning algorithm on IoT quality sensor dataset [4]. Baowei et al. developed an IoT device for air quality forecasting with interactive decision-making tool [5]. Liang et al. developed an IoT-based air quality monitoring device based on the communication interface [6]. Saba et al. analysed various machine learning algorithms used for predicting air quality in smart cities [7]. Kan et al. developed low power wide area technology to use in an air quality monitoring system [8].

Carlos et al. developed event-based sensing on IoT node power efficiency calculation for performing air quality monitoring [9]. Bin et al. developed a low cost and effective electrochemical gas sensor for environmental monitoring [10]. Swati et al. developed an air quality index to predict air quality [11]. Mario et al. developed a particulate matter sensor to analyse and monitor air quality [12]. Ayele and Mehta developed a recurrent neural network with IoT for air quality monitoring [13]. Rasha built an air quality monitoring and warning system [14]. Sharafat et al. developed an infra red sensor for air quality monitoring [15]. Zhbin et al. developed a multipoint air quality monitoring system [16]. Zhang and Woo developed Real Time Localized Air Quality Monitoring and Prediction Through Mobile and Fixed IoT Sensing Network [17]. Firdhous et al. developed IoT Enabled Proactive Indoor Air Quality Monitoring System for Sustainable Health Management [18]. Quang et al. developed Sensing Data Fusion for Enhanced Indoor Air Quality Monitoring [19]. Kinnera Bharath et al. developed Arduino and MQ Series Sensors With Dataset Analysis [20].

14.3 Methodology

In the proposed system, the atmospheric gases are measured using Smart citizen kit. Smart Citizen kit consists of two boards Sensor Board and Data Board. Sensor

Board senses Temperature, Humidity, Carbon Monoxide, Nitrogen Dioxide, Light and Noise sensor. Data Board comprises of WiFi module, Battery, Real Time Clock, and Solar Panel connector for using the smart citizen kit in outdoors. Initially, the firmware of the smart citizen kit needs to be updated using the microUSB, and Arduino ISP sketches need to be uploaded to Arduino IDE. SCK Wifi commands are used to set the SSID, phrase and Authentication of the Internet connected. Using the power supply Sensor Board senses the atmospheric gases and communication is done through the WiFi module present in Data Board. The sensed data from the smart citizen kit will be posted to the Serial monitor and to the smart citizen kit server. In the Smart citizen kit server the kit details and location, MAC address need to be provided by the owner of kit and the data will be posted in the server.

The posted data can be downloaded from the smart citizen website in the csv format. The dataset can also be collected in the polluted areas. From the dataset collected the input parameters are Temperature, Humidity, Carbon Monoxide, and Nitrogen Dioxide. Curve Fittings are used to predict the data where no data is present. Using the curve fittings the data can be visualized and identify the relation between dependent and independent parameter. The curve fitting is for finding the optimized solution from the set of input parameters.

From the curve fitting the data can be visualized and relation can be identified between both dependent and independent variables in python. Several libraries like Numpy, Matplotlib, NumPy for array data structure, Matplotlib to plot data are used in python for curve fitting. Linear Regression is used to predict the Carbon Monoxide and curve be fitted for observed and predicted. The curve is plotted for dependent and independent variable where independent variable is the observed variable and predicted is the dependent variable. Linear Regression uses equation $y = m \cdot x + c$ to predict the Carbon Monoxide level dependent variable with data collected. Figure 14.1 shows the methodology of the proposed method.

14.3.1 Input

The input to the system is the atmospheric gas. The Smart citizen kit version 1.1c senses the atmospheric Carbon Monoxide, Nitrogen Dioxide using Gas sensor, Temperature Humidity, Light and Noise level in its surroundings.

14.3.2 Smart Citizen Kit

Smart citizen kit is the set of Hardware Component that provides in monitoring the environmental changes. Smart citizen kit contains two boards Urban Sensor board and Data Board. Smart citizen kit allows to measure the Temperature, Light, Carbon Monoxide, Nitrogen Dioxide and Humidity and can be monitored anywhere in the world.

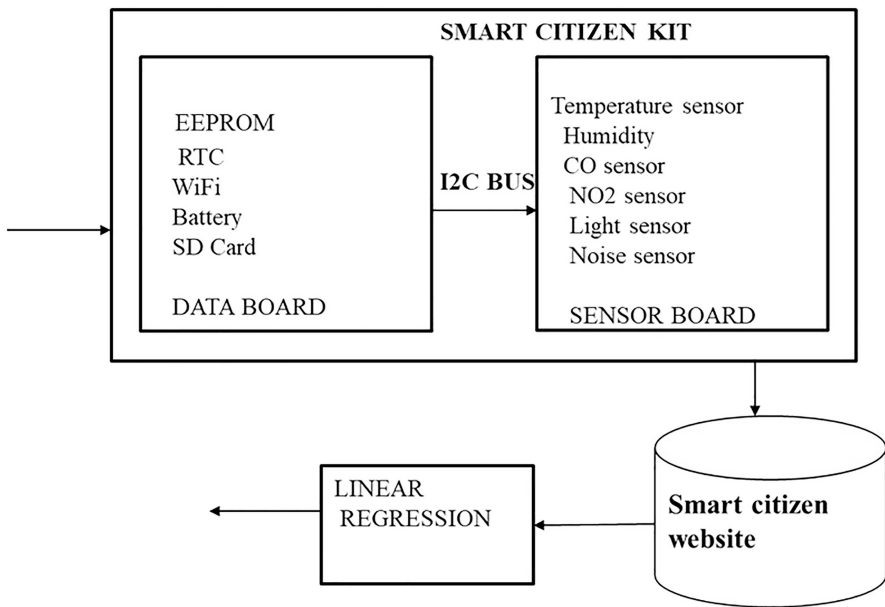


Figure 14.1 The flow diagram of air quality monitoring system.

14.3.2.1 Sensor Data

Sensor board the power supplied to sensor will be 3.3 V and sensors are Temperature, Humidity, Gas Sensor, Light and Noise Sensor. Gas sensor will sense Carbon Monoxide and Nitrogen Dioxide. It also contains Vcc, 3.3 V, and several pins. The Sensor board is shown in Figure 14.2.

14.3.2.2 Data Board

Data Board contains Battery, WiFi module to communicate the sensor data collected from the atmosphere, Solar Panel can be connected if the kit is to maintain outdoor atmospheric gas level. Real Time Clock RTC is to keep track time. SD card is used to store the sensed data when the kit is offline. EEPROM memory is also used to store data when the kit is disconnected to Internet. The data board is shown in Figure 14.3.

14.3.3 Smart Citizen Website

In the Smart citizen website, the kit details need to be configured using the Mac address of the kit and the location of kit in www.smartcitizen.me website. The firmware needs to be updated smart citizen kit consists of two parts one is done by

Arduino UNO microcontroller and other is AVRISP MKII. After burning the Bootloader using ArduinoISP sketches the firmware can be updated and giving the power supply to Data Board of smart citizen kit the sensed data from the atmosphere will be posted to the smart citizen server and posted data can be downloaded in csv format.

14.3.4 Curve Fitting

The data sensed from the kit in the location like parking and industrial areas will be varying. Based on the variation of atmospheric gases the curve fitting is applied to the dataset on comparing Carbon Monoxide and Nitrogen Dioxide data. Curve fittings are done using linear regression. Increasing the dataset increases the accuracy of prediction of atmospheric gas level.

14.3.5 Prediction of Gas

The output of the curve fittings will be given as input to the prediction of atmospheric gas. Based on the gas level and curve the prediction of Carbon Monoxide will be done using linear regression. From the linear regression, the curve is plotted between Carbon Monoxide observed and predicted values.

The linear regression curve is fitted by plotting the observed independent variable and the predicted dependent variable from fitting the linear regression curve to the observed independent variable and the intercept will be the prediction of Carbon Monoxide level in atmosphere.

14.4 Results and Discussion

14.4.1 Sensing the Air Quality

Air quality sensing is done with the help of Smart Citizen Kit (v1.1). It has two boards Data board and the Sensor board. The sensor board has sensors for measuring NO₂, CO gases, Light, Noise level, Temperature, and Humidity. These are the steps to be followed for installation of the kit: (Figure 14.4)

- Sign Up
- Adding kit to the platform
- Registration of kit using mac

Sign Up:

Adding kit in the Platform:

After login new kit is added. For others to understand the kit better, a name, location, and description are added for the kit. Location can be adjusted by

Sign up ✕

Join Smart Citizen

Username *

Username is required

Password *

Email *

☐ I have read and accept Terms and Conditions

ALREADY HAVE AN ACCOUNT? LOG IN

Figure 14.4 Sign up page.

dragging marker in the map. Kit exposure is also added which is either indoor or outdoor. The kit can be monitored globally in the map as shown in Figure 14.5.

Registering the kit in the platform:

Chrome extension for smart citizen kit is added and the app is downloaded. After this, the kit is logged in with the registered mail id and the password. In order to register the kit, the MAC address of the kit is saved as shown in Figure 14.6. The MAC address of the kit is found either in the wifi module or by using the SCK command “get mac”. “###” is the command to wake up the SCK command mode. This is done after setting the baud rate to 115200 in the Arduino IDE (Figure 14.6).

14.4.2 Posting Data to the Website

The following steps are done in order for the sensed data to get posted on the smartcitizen.me website and the dataset is downloaded in the csv format for further analysis of sensed data. The steps followed are as follows:

- Firmware Updation.
- Burning bootloader.
- Configuring the WiFi settings.
- Uploading code and downloading collected data.

Sign up

×

Join Smart Citizen

Username *

Username is required

Password *

Email *

☐ I have read and accept Terms and Conditions

ALREADY HAVE AN ACCOUNT? LOG IN

Figure 14.5 Locating the kit in map.

Setup your kit

In order to have your kit connected to the Smart Citizen platform, we need a few step involving the connection of your kit to your computer. This tool will help you register your kit to the platform, settings and update its firmware. Currently we support Google Chrome in Win, Mac and Linux. If this is your first time, maybe you will like to follow the [Startup guide](#).

Powered by BabelFish technology by Codebender.

Sorry, currently we just support Google Chrome for configuring your Smart Citizen Kit. You can download it [here](#)

Mac address

Mac Address

00:06:66:35:87:d2

The setup tool will read the Mac Address automatically from your kit. Please wait or enter it manually.

SAVE

Figure 14.6 Registering the kit.

Firmware Updation:

The latest version of the firmware is downloaded. Firmware is updated using Arduino IDE. For updating it, the firmware is edited and it is uploaded to the kit. Any number of wifi networks can be added with their SSID and password which can not be longer than 32 characters. The wifi configuration mode is chosen as WPA2 for both the networks. Internal antenna is chosen as default. This is the firmware updation. More than one wifi networks is separated with comma. Code is uploaded after editing the firmware. In case if port is not available, bootloader should be burned. The wifi configuration can also be done manually using Wifly commands.

Burning bootloader:

Arduino is turned into AVR ISP to burn the bootloader to the SCK. Bootloader is the small piece of code running inside the smart citizen kit. It can be programmed and configured over USB. Bootloader should be reinstalled if it is crashed. If USB/ Serial port is not visible, then the bootloader is crashed. For this the Arduino is wired with SCK as shown in Figure 14.8 Then the following should be selected. After sometime bootloader burning will be done (Figures 14.7 and Figure 14.8).

Tools > Board > Arduino LilyPad USB

Tools > Programmer > Arduino as ISP

Tools > Burn bootloader

Configuring the WiFi Settings:

The wifi configuration is done and it can be changed using SCK Wifly commands. First \$\$\$ command is typed in the serial monitor to wake up the

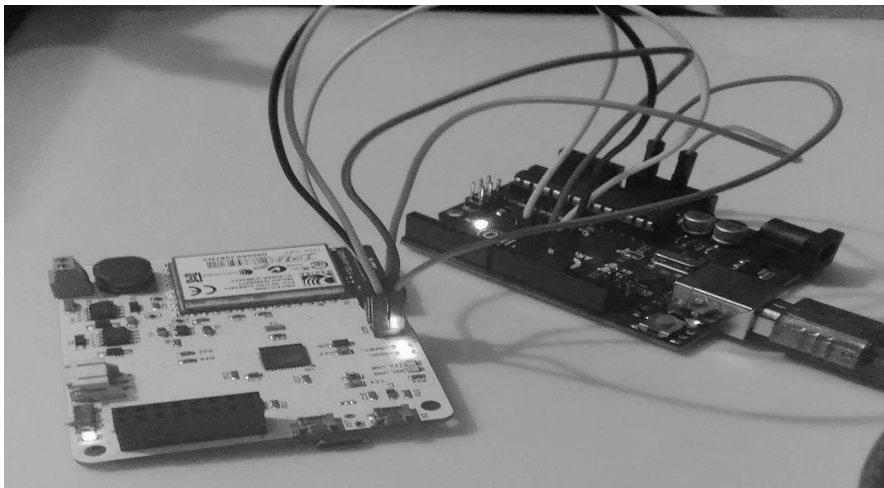


Figure 14.7 Burning the bootloader.

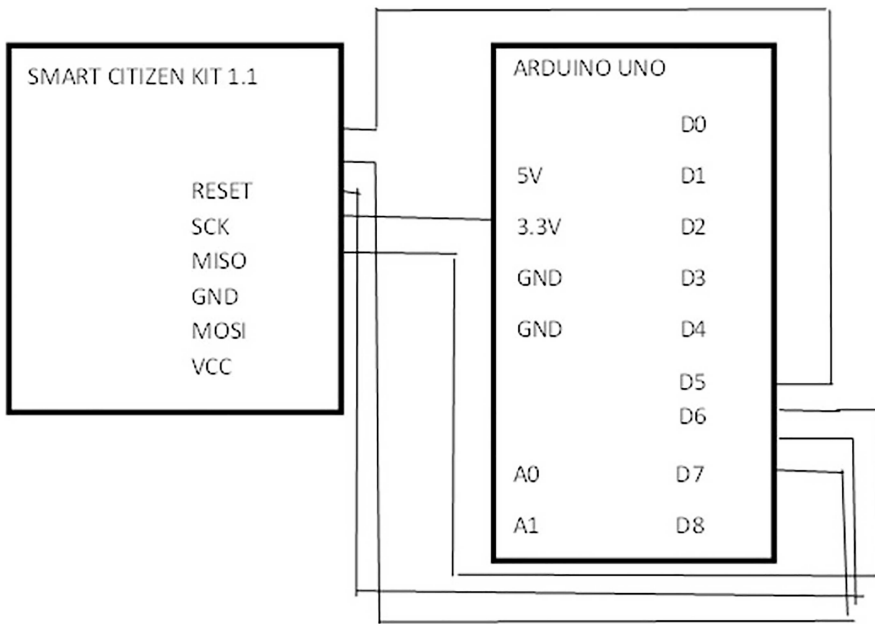


Figure 14.8 Circuit diagram for connecting Arduino and SCK.

module and to activate the Wi-fi command mode. The following steps are done after that

set wlan ssid xxx

The xxx in the command is replaced by the corresponding ssid

set wlan phrase xxx

xxx is replaced with password for the ssid given above

set wlan auth X

This adds the authentication to the memory. X is replaced with

“0” for open, “1” for WEP, “2” for WPA1, “4” for WPA2 and “6” for WEP64

Exit

This goes to the normal operational mode

Now the set up ssid and password is checked by waking up the SCK module

###	-To wake up SCK module
get mac	-get the mac address of the kit
get wlan ssid	-to get the ssid saved on the kit
get wlan phrase	-to get the phrase saved on the kit
clear nets	-This clears all the saved WiFi configuration

information	
get wlan auth	-to get the authentication method saved on the kit.
get all	-to retrieve all the settings saved on the kit.

14.4.3 Uploading and Downloading Data

On the Arduino IDE, LilyPad USB is selected from tools menu. Now the upload button is clicked and the code is uploaded and the data is published in the smartcitizen.me website. We can check data coming in the Arduino serial monitor. It can also be used to check whether everything is ok. In case of WiFi connection failure, it should look as if this can be solved by checking WiFi connection. If network failure occurs, then the collected data will get posted once internet connection is established again. Now the data posted in the website is downloaded in the csv format which is done by clicking the download csv button in the website. The data collected for the particular time stamp is used for further analysis i.e., to plot the curve using curve fitting model. The url of the registered is <https://smartcitizen.me/kits/13829> which can be accessed from anywhere in the world by anyone.

14.4.4 Prediction Using Linear Regression

Prediction is done from fitting the curve from the dataset posted in the website or dataset collected based on the pollution level in atmosphere in the vehicle count and the steps involved are as follows:

- Importing the Libraries and Read Independent variable.
- Visualizing and fitting Linear Regression.
- Predicting the gas level.

14.4.5 Importing the Libraries and Read Independent Variable

The first step is to import the required library using pip installer. The libraries used are Numpy and Matplotlib. Numpy library function is used to store array values as it uses continuous memory location and it works fast. Matplotlib library function is used to visualize the datasets.

Pip commands to install the library are `pip install numpy`
`pip install matplotlib`

Linear Regression is the model with the relationship between independent and dependent variables. In the linear regression, it contains one input parameter and

one output parameter the input parameter is the independent variable where dependent variable is the output variable. From the dataset, the feature will be extracted i.e., independent variable.

14.4.6 Visualizing and Fitting Linear Regression

Using the matplotlib, pyplot library function the dataset can be used to visualize the data. The scatter function is used to draw datapoint for both x and y axis that is denoted in circle. plot function is used to draw line to visualize. Curve fitting is used to find the optimized dependent variable and using the linear regression the predicted data will be fit to equation of linear regression.

14.4.7 Predicting the Gas Level

The result of linear regression will be plotted for observed and predicted variable. The linear regression is the equation for line $y = m \cdot x + c$ it is the linear model the predicted value will be plotted as linear data. First step is to load the dataset file and retrieve the required independent variable. Next, calculate the mean for independent variable from the dataset and find the predicted value using linear regression curve

14.4.8 Input

The atmospheric gases like Carbon Monoxide, Nitrogen Dioxide, Temperature, Humidity, Light and Noise levels are sensed by smart citizen kit. The sensed data from smart citizen kit will also displayed in Serial Monitor as shown in Figure. Air Quality data is collected for Carbon Monoxide level based on the vehicle count in the parking area of Mepco Schlenk Engineering College during 4 pm to 6 pm and 8.15 am to 9.30 am (Figures 14.9 and 14.10).



Figure 14.9 Atmospheric pollution.

```

*****
Temperature: 28116 C RAW
Humidity: 17120 % RAW
Light: 39.00 lx
Battery: 100.00 %
Solar Panel: 0 mV
Carbon Monoxide: 83.86 kOhm
Nitrogen Dioxide: 9.50 kOhm
Noise: 1572 mV
Wifi Spots: 4
UTC: 2021-3-17 06:49:09
*****
SCK Waking up...
SCK Connected!!
updates = 1
Posted to Server!
Old connection active. Closing...
SCK Sleeping
*****
Temperature: 28108 C RAW
Humidity: 17048 % RAW
Light: 39.00 lx
Battery: 100.00 %
Solar Panel: 0 mV
Carbon Monoxide: 85.96 kOhm
Nitrogen Dioxide: 9.59 kOhm
Noise: 1465 mV
Wifi Spots: 4
UTC: 2021-3-17 06:50:05
*****
SCK Waking up...

```

Figure 14.10 Sensed data in serial monitor.

14.4.9 Sending Data to Website

The sensed data will be displayed as graph in the website to visualize the gas level and can be downloaded from the Smart citizen platform (Figure 14.11).

14.4.10 Prediction of Gas Using Linear Regression

The result from the smart citizen kit be collected in the dataset. Using the Curve fitting the dataset characteristic is fitted with linear regression curve the observed

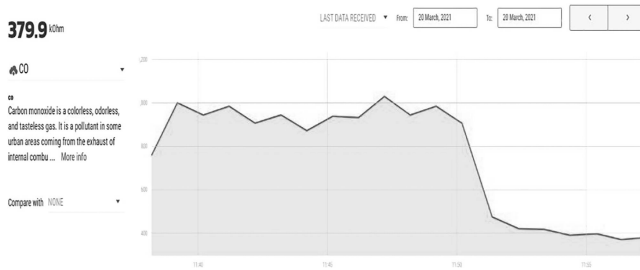


Figure 14.11 Gas level shown in website.

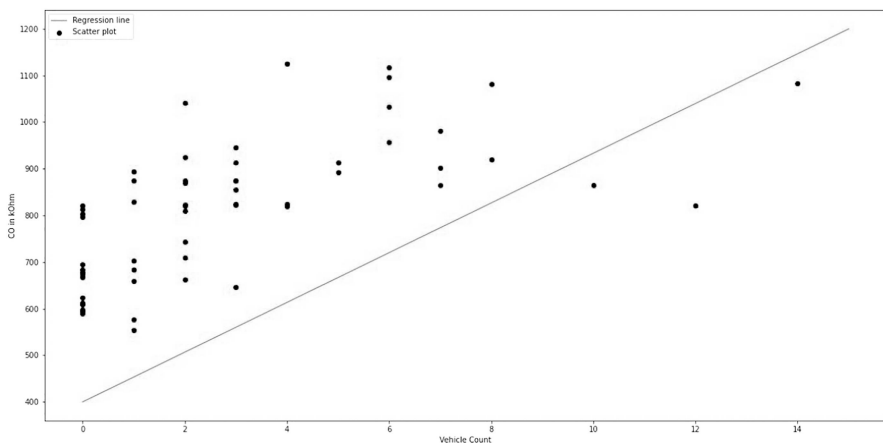


Figure 14.12 Prediction of Carbon Monoxide.

(independent variable) and predicted(dependent variable) of Carbon Monoxide values are inferred using linear regression (Figure 14.12).

Finally the result from the curve fitting using the linear regression will be the prediction of Carbon Monoxide.

14.5 Conclusion

The proposed system detects the air quality using the Smart citizen kit and also predicts the atmospheric Carbon Monoxide levels. The Smart citizen kit measures the Temperature, Humidity, Carbon Monoxide, Nitrogen Dioxide, Light and Noise. With the help of WiFi module in Data Board the sensed data will be posted to Smart citizen server over Internet or else in offline mode an SD card can be used. From the dataset, the curve fitting is applied to find the optimized parameter for observed independent variable vehicle count and predicted dependent variable. Carbon Monoxide levels in atmosphere using the linear regression and predict Carbon Monoxide levels.

References

1. Camprodon, G., González, Ó., Barberán, V., Pérez, M., Smári, V., de Heras, M. Á., & Bizzotto, A. (2019). Smart citizen kit and station: An open environmental monitoring system for citizen participation and scientific experimentation. *HardwareX*, 6, e00070.
2. Huang, J., Duan, N., Ji, P., Ma, C., Ding, Y., Yu, Y., ... & Sun, W. (2018). A crowdsourcing-based sensing system for monitoring fine-grained air quality in urban environments. *IEEE Internet of Things Journal*, 6(2), 3240–3247.
3. Becnel, T., Tingey, K., Whitaker, J., Sayahi, T., Lê, K., Goffin, P., Butterfield, A., Kelly, K., & Gaillardon, P. E. (2019). A distributed low-cost pollution monitoring platform. *IEEE Internet of Things Journal*, 6(6), 10738–10748.
4. Gambi, E., Temperini, G., Galassi, R., Senigaglia, L., & De Santis, A. (2020). ADL recognition through machine learning algorithms on IoT air quality sensor dataset. *IEEE Sensors Journal*, 20(22), 13562–13570.
5. Wang, B., Kong, W., Guan, H., & Xiong, N. N. (2019). Air quality forecasting based on gated recurrent long short term memory model in Internet of Things. *IEEE Access*, 7, 69524–69534.
6. Zhao, L., Wu, W., & Li, S. (2019). Design and implementation of an IoT-based indoor air quality detector with multiple communication interfaces. *IEEE Internet of Things Journal*, 6(6), 9621–9632.
7. Ameer, S., Shah, M. A., Khan, A., Song, H., Maple, C., Islam, S. U., & Asghar, M. N. (2019). Comparative analysis of machine learning techniques for predicting air quality in smart cities. *IEEE Access*, 7, 128325–128338.
8. Zheng, K., Zhao, S., Yang, Z., Xiong, X., & Xiang, W. (2016). Design and implementation of LPWA-based air quality monitoring system. *IEEE Access*, 4, 3238–3245.
9. Santos, C., Jiménez, J. A., & Espinosa, F. (2019). Effect of event-based sensing on IoT node power efficiency. Case study: Air quality monitoring in smart cities. *IEEE Access*, 7, 132577–132586.
10. Tian, B., Hou, K. M., Diao, X., Shi, H., Zhou, H., & Wang, W. (2019). Environment-adaptive calibration system for outdoor low-cost electrochemical gas sensors. *IEEE Access*, 7, 62592–62605.
11. Dhingra, S., Madda, R. B., Gandomi, A. H., Patan, R., & Daneshmand, M. (2019). Internet of Things mobile–air pollution monitoring system (IoT-Mobair). *IEEE Internet of Things Journal*, 6(3), 5577–5584.
12. Diván, M. J., Sánchez-Reynoso, M. L., Panebianco, J. E., & Méndez, M. J. (2021). IoT-based approaches for monitoring the particulate matter and its impact on health. *IEEE Internet of Things Journal*, 8(15), 11983–12003.
13. Ayele, T. W., & Mehta, R. (2018, April). Air pollution monitoring and prediction using IoT. In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)* (pp. 1741–1745). IEEE.
14. AbdulWahhab, R. S. (2020, September). Air quality monitoring system: Towards IoT-based system for air pollutant concentration prediction. In *2020 10th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 311–316). IEEE.
15. Ali, S., Glass, T., Parr, B., Potgieter, J., & Alam, F. (2020). Low cost sensor with IoT LoRaWAN connectivity and machine learning-based calibration for air pollution monitoring. *IEEE Transactions on Instrumentation and Measurement*, 70, 1–11.

16. Liu, Z., Wang, G., Zhao, L., & Yang, G. (2021). Multi-points indoor air quality monitoring based on Internet of Things. *IEEE Access*, 9, 70479–70492.
17. Zhang, D., & Woo, S. S. (2020). Real time localized air quality monitoring and prediction through mobile and fixed IoT sensing network. *IEEE Access*, 8, 89584–89594.
18. Firdhous, M. F. M., Sudantha, B. H., & Karunaratne, P. M. (2017, February). IoT-enabled proactive indoor air quality monitoring system for sustainable health management. In *2017 2nd International Conference on Computing and Communications Technologies (ICCCCT)* (pp. 216–221). IEEE.
19. Ha, Q. P., Metia, S., & Phung, M. D. (2020). Sensing data fusion for enhanced indoor air quality monitoring. *IEEE Sensors Journal*, 20(8), 4430–4441.
20. Sai, K. B. K., Mukherjee, S., and Sultana, H. P. (2019). Low cost IoT based air quality monitoring setup using Arduino and MQ series sensors with dataset analysis. *Procedia Computer Science*, 165, 322–327.

Chapter 15

Smart Shoes for Vision Disabled

Janhvi Mishra¹ and Divyanshu Tiwari²

¹*Christ University, Pratapgarh, Uttar Pradesh, India*

²*Sidharth University, Gorakhpur, Uttar Pradesh, India*

15.1 Introduction

The power of vision plays a crucial role in human physiology, as our eyes enable us to perceive and interact with the world around us. However, there are approximately 285 million people worldwide who are visually impaired, and around 39 million of them being blind, as the survey done by the World Health Organization (WHO). What's even more concerning is that 80% of the blind population is aged 50 or above.

To address this issue, an innovative solution is proposed: A shoe specifically designed to assist blind individuals in navigating their surroundings with greater confidence and safety. The shoe incorporates various technologies, including Arduino (UNO, NANO) microcontrollers, ultrasonic sensors, fire detection sensors, vibration sensors, a beeper, and a tracker. By utilizing these components, the shoe aims to enhance the mobility and independence of visually impaired individuals, particularly when they venture into unfamiliar environments.

The inclusion of an ultrasonic sensor within the shoe serves to detect obstacles in the user's path, providing a warning through either a beeping sound or vibrations. This real-time feedback allows the wearer to remain alert and greatly reduces the likelihood of accidents or collisions. Furthermore, a fire detection sensor is integrated

into the shoe, enabling it to identify the presence of fire in the vicinity and promptly alert the user.

This feature ensures that blind individuals can quickly evacuate potentially dangerous areas.

Additionally, the shoe incorporates a tracker, which proves immensely valuable to the family members or caregivers of the visually impaired. This tracking functionality helps locate the individual in case they become disoriented or lose their way, which can often happen due to the absence of visual cues. By providing information about the wearer's current location, the system offers peace of mind and ensures prompt assistance if needed.

The primary objective of this system is to provide an efficient navigation aid for blind individuals, effectively granting them a sense of vision by conveying vital information about their surroundings and nearby objects. By leveraging the power of technology and incorporating it into footwear, this innovative solution aims to empower the visually impaired, enabling them to explore and navigate the world with increased confidence, independence, and safety.

15.2 Smart Devices and Their Use in Our Project

Individuals who are blind or visually impaired often encounter challenges when traveling in unfamiliar environments, as they lack sufficient information about their location, traffic conditions, and obstacles that are easily perceivable by those without visual impairments. However, in today's technological landscape, there are various solutions available, such as GSM (Global System for Mobile Communications) and GPRS (General Packet Radio Service), that aid blind individuals in navigating their surroundings.

Blind people are fully capable of leading normal lives, albeit with their own unique ways of doing things. However, when it comes to walking outside their homes, they frequently encounter obstacles due to inaccessible infrastructure and social barriers. To address these challenges and improve their quality of life, it is crucial to provide them with effective assistance.

Technologies such as GSM and GPRS can play a significant role in this regard. These technologies utilize mobile networks to transmit data, enabling blind individuals to access real-time information about their surroundings, including traffic conditions and potential obstacles. This information empowers them to navigate unfamiliar places more confidently and safely.

By leveraging these technologies, blind individuals can receive location-based updates, directions, and alerts on their mobile devices or specialized assistive devices. These tools can inform them about nearby points of interest, public transportation options, accessible routes, and potential hazards. Furthermore, integration with navigation applications or voice-assisted systems can provide step-

by-step directions and audio cues, facilitating independent travel and reducing reliance on others for guidance.

Moreover, addressing the issue of inaccessible infrastructure is crucial to ensuring the ease of travel for blind individuals. It requires collaborative efforts between policymakers, urban planners, and architects to create inclusive environments with tactile paving, audible signals at intersections, and proper signage. Additionally, raising awareness about the challenges faced by blind individuals and fostering a more inclusive and empathetic society can help overcome social barriers.

By harnessing technologies like GSM and GPRS, coupled with accessible infrastructure and increased societal awareness, we can make significant strides in improving the lives of blind and visually impaired individuals. These advancements will enable them to navigate unfamiliar places with greater ease, independence, and safety, thereby fostering inclusivity and empowering them to live their lives to the fullest.

15.2.1 Devices Required

- Arduino (UNO, NANO)
- Ultrasonic sensor
- Fire Detection sensor
- Vibration sensor
- Beeper
- Tracker

15.2.2 Arduino (UNO, NANO) Arduino Uno

The Arduino Uno is a microcontroller board that was designed to be open-source and released in 2010. It is built around the Microchip ATmega328P microcontroller and is equipped with sets of digital and analog input/output (I/O) pins that allow users to interface with various expansion boards and other circuits which are used. Arduino board has approximated 14 digital input/output (I/O) pins, 6 of which are capable of Pulse-Width Modulation output, and 6 analog input/output (I/O) pins.

Arduino Uno can be programmed using the Arduino Integrated Development Environment (IDE), it is a free software application used to write and upload code to the board. The Integrated Development Environment (IDE) is available on the Arduino website, and users can write their own programs or use pre-made code available in the Arduino community. The board is programmed via a USB cable of type B, which is included with the board.

Arduino Uno can be powered using USB cable or an external 9-volt battery. The Arduino board can accept voltages between 7 and 20 volts, which makes it compatible with a wide range of power sources. This flexibility allows users to choose the most suitable power source for their project.

The Arduino Uno is similar to other Arduino boards, such as Arduino Nano and Leonardo, which also have similar features and capabilities. Hardware reference design of the board is distributed under a Creative Commons Attribution Share-Alike 2.5 license, which means that users are free to use, modify, and distribute the design as long as they credit the original creator and share their modifications under the same license. Additionally, there is an availability of layout and production files for some versions of the hardware, which makes it easier for users to manufacture their own boards or modify existing ones. Overall, the Arduino Uno is a versatile and the most popular microcontroller board that is used in the maker and DIY communities.

The term “uno” is an Italian word that translates to “one” in English. This particular name was selected to signify a significant redesign of both the Arduino hardware and software.

15.2.3 General Functions of the Pins Used

- **LED:** The Arduino Uno has a number of pins that serve different functions. One of these is the Led, which is built-in and controlled by digital pin 13 in Figure 15.1. When value becomes high in the pins, the Led turns on and when the value becomes low, it turns off (Figure 15.2).
- **VIN:** Another important pin is the VIN pin (Voltage In), which is basically used to the board to input voltage when an external power source is being used. This can be done either by supplying voltage through the VIN pin directly or through the power jack, which can then be accessed through the VIN pin.

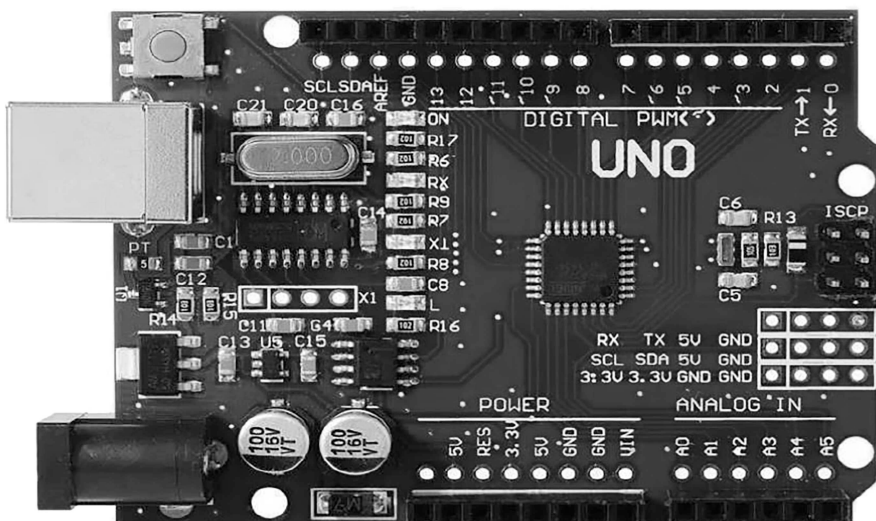


Figure 15.1 Arduino UNO chip.

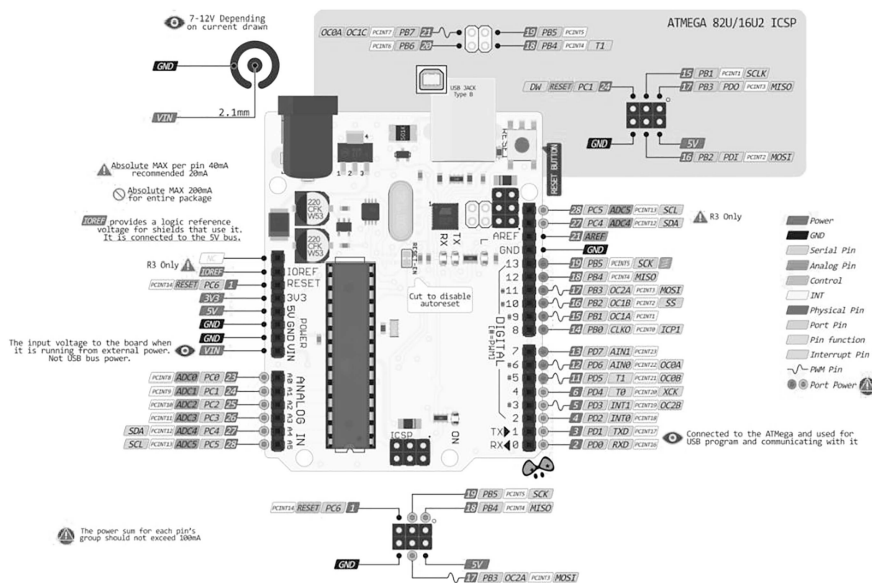


Figure 15.2 Arduino UNO pinout diagram.

- **5 V:** The board also has a 5 V pin, which is being used to supply power to arduino also which results in the on-board regulator as regulated 5 V. The power jack (7-20 V), the USB connector (5 V), or the VIN pin (7-20 V) can provide the power to the board. However, the damage can occur to the board if the supply of voltage through the 5 V or 3.3 V pins bypasses the regulator.
- **3V3:** Another pin is the 3V3, which provides the supply of 3.3-volt on on-board regulator in the arduino, and the maximum current draw is 50 mA for 3V3 pin.
- **GND:** GND represents ground pins in arduino UNO.
- **IOREF:** IOREF pin is a pin present in arduino UNO which provides the voltage reference for the microcontroller's operation.
- **Reset:** Finally, there is the reset pin. It is used to add a reset button to block the one on the board. All of these pins serve important functions and are integral to the operation of the Arduino Uno board.

15.2.4 Special Pin Functions

The Arduino Uno uses pins for input and output. There are 6 analog pins and 14 digital pins that can be used, which provide control through software using pin Mode (), digital Write (), and digital Read () functions. These pins contain 5 volts of voltage for operating, and each can receive or provide up to 20 mA. It is important not to exceed 40 mA on any I/O pin as if it exceeds, there are chances

that microcontroller can get damaged permanently. The Arduino Uno also features six analog inputs, which are labeled “A0” through “A5”, and each provides ten bits of resolution, giving 1024 different values. By default, these inputs measure from 0 volts to 5 volts, but using the AREF pin the upper end of the range can be changed and the analog Reference () function.

15.2.5 Specialized Functions of the Pins

- **Serial or UART:** In addition to the general pin functions described earlier, the Arduino Uno board has several special pins with specific functions.
- **External interrupts:** Pins 2 and 3 can be used for external interrupts and can be configured to trigger an interrupt on a low value, rising or falling edge, or a change in value.
- **PWM:** The board also has six pins that support pulse-width modulation of pins like 3, 5, 6, 9, 10, and 11, which can provide 8-bit PWM output using the analog Write () function.
- **SPI:** Another pin is the SPI pins (10, 11, 12, and 13), SPI stands for Serial Peripheral Interface communication using the SPI library.
- **TWI or I²C:** The TWI or I²C pins are the Two-Wire Interface communication which uses the Wire library.
- **AREF:** AREF pin provides the reference voltage for analog inputs, using the analog Reference () function reference voltage can be changed. These special pins offer greater flexibility and functionality to the Uno board, making it a versatile tool for various projects.

15.2.6 Arduino Nano

The **Arduino Nano** was introduced in 2008 as a compact and fully functional board based on the ATmega328P. Its form factor is smaller than that of Arduino “Uno” but offers similar connectivity and specifications. The Nano features 30 male I/O headers arranged in a DIP-30 configuration and with the help of Arduino Software IDE, they can be programmed. IDE is very common for all types of Arduino boards and can be used online as well as offline. Power can be supplied to the board via a type-B mini-USB cable or a 9 V battery. Compared to the Uno, the Nano does not have a DC power jack and uses a Mini USB port instead of a USB B port. Additionally, the Nano employs a USB-TTL converter chip. Overall, the Arduino Nano is a breadboard-friendly version of the Uno that is smaller in “size” but still offers many of the same features and functionalities (Figure 15.3).

15.2.7 Ultrasonic Sensor

Ultrasonic sensors are also known as level sensors, which are helpful in determining the distance measurements with the help of ultrasonic waves. These sensors emit an

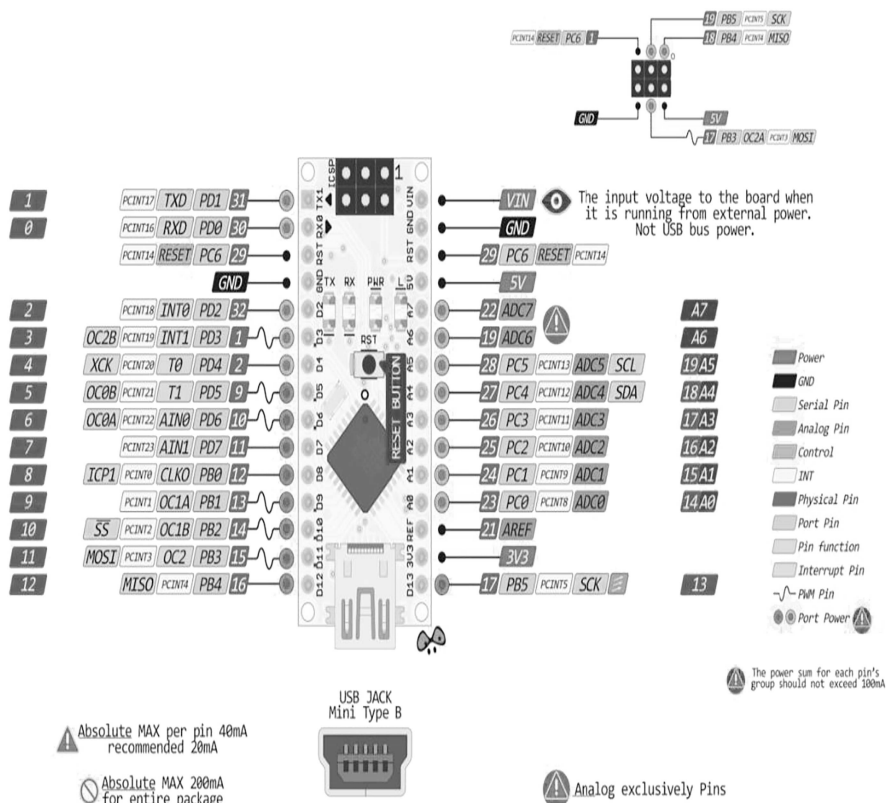


Figure 15.3 Arduino NANO pinout.

ultrasonic wave and receive the wave that is reflected back from the target object. By measuring the time between the emission and reception, ultrasonic sensors are able to determine the distance to the target. Essentially, an ultrasonic sensor works by emitting ultrasound and then detecting the reflected wave to determine the distance of an object. This type of sensor is commonly used for detecting objects and measuring distances in a variety of applications. Overall, ultrasonic sensors are an effective tool for measuring distances and detecting objects by utilizing the properties of ultrasonic waves (Figure 15.4).

15.2.8 Ultrasonic “Waves”

Ultrasonic waves are basically sound waves that have the frequency higher than the limit of human hearing. To generate and detect these waves, specialized microphones called transducers are used. Ultrasonic sensor modules such as the HC-SR04 employ a single transducer to both emit an ultrasonic pulse and receive the echo that is reflected back from a target object similarly as ultrasonic sensors.



Figure 15.4 Ultrasonic “sensor”.

The distance between the sensor and the object is calculated by calculating the time taken by the waves to come back after reflecting from the object. The speed of sound in air is used to determine the distance traveled by the ultrasonic wave. Sensor module sends out a pulse of ultrasonic sound and then waits for the echo to return. By measuring the time difference between the moving and coming back of the pulse, the distance to the object can be calculated. This measurement process is repeated continuously at regular intervals to provide accurate and real-time distance measurements. Overall, ultrasonic sensor modules make use of transducers to generate and detect ultrasonic sound pulses, which are then used to calculate distance measurements based on the time delay between transmission and reception.

$$\text{distance} = \frac{\text{speed of sound} \times \text{time taken}}{2}$$

15.2.9 To Interface an Ultrasonic Sensor

The HC-RS04 Ultrasonic sensor module features four pins: VCC, GND, TRIG, and ECHO. VCC and GND pins are used for power supply, while the TRIG pin is utilized for transmitting ultrasonic sound waves and the ECHO pin is employed for receiving them. To interface the HC-RS04 sensor module with an evive board, the following connections should be made (Figure 15.5):

- It connects the VCC pin of the sensor module to the VCC pin of the evive board.

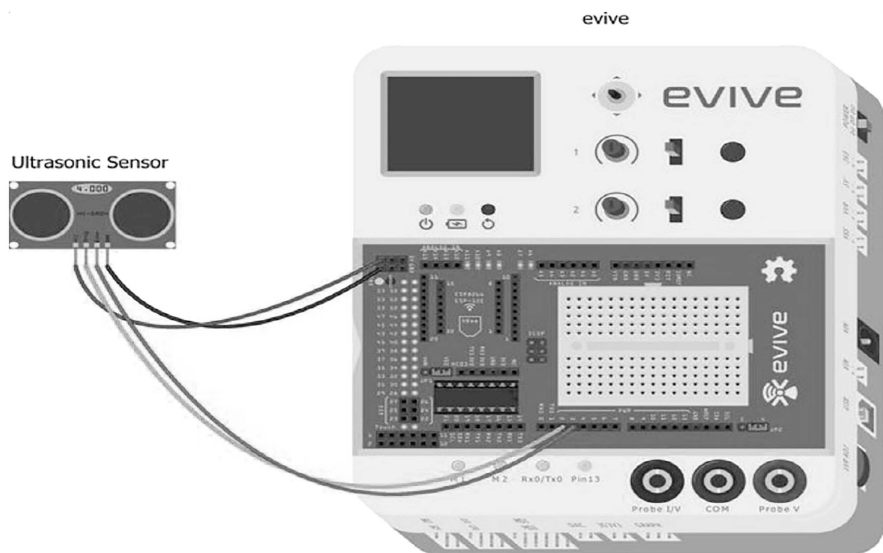


Figure 15.5 Ultrasonic “sensor”.

- It connects the GND pin of the sensor module to the GND pin of the evive board.
- It connects the TRIG pin of the sensor module to digital pin 2 of the evive board.
- It connects the ECHO pin of the sensor module to digital pin 3 of the evive board.

This setup enables the evive board to send and receive ultrasonic sound waves, and by measuring the time delay between transmission and reception, calculate the distance between the sensor module and a target object. By following these steps, the HC-RS04 sensor module can be easily interfaced with an evive board for a variety of applications, including “distance” measurement and object detection.

15.2.10 Fire Detection Sensor

A fire detection system is a mechanism or device designed to identify the presence of combustion or its by-products and trigger an alarm or signal, which could be audible, visual, or in any other form. This includes all equipment utilized to transmit fire alarm activations and related signals to a distant location. The purpose of a fire detection system is to alert occupants of a building or facility to the presence of fire, smoke, or other hazardous conditions, allowing them to evacuate quickly and safely. These systems can be installed in homes, commercial buildings, factories, and other public spaces. By detecting fire or

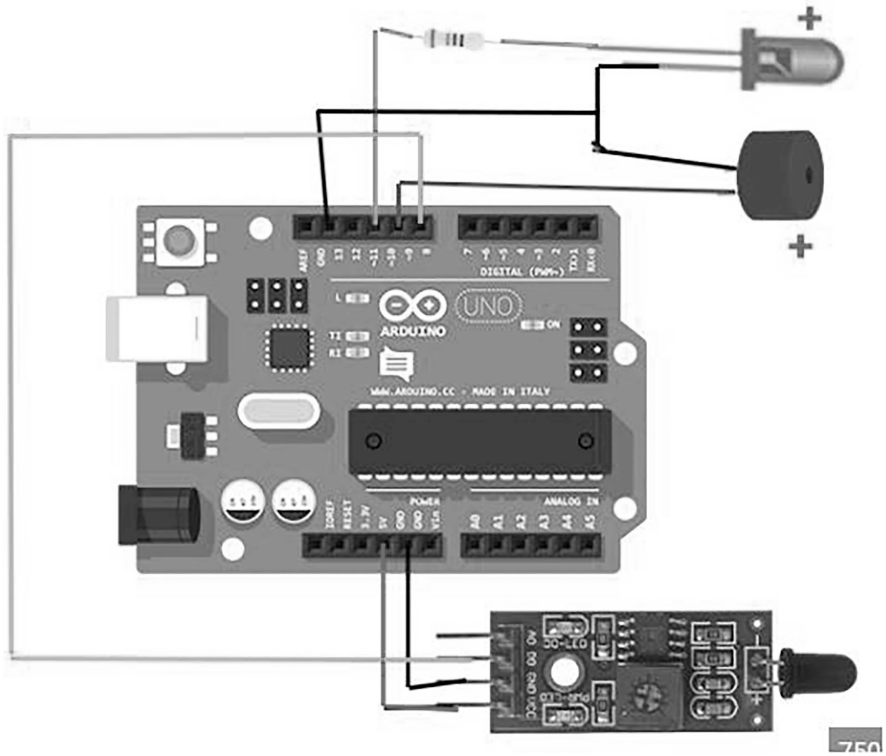


Figure 15.6 Fire detector sensor.

smoke early, fire detection systems can help prevent property damage, injuries, and even fatalities (Figure 15.6).

15.2.11 Vibration Sensor

A vibration sensor is an electronic device which is designed to calculate the magnitude and frequency of vibration in a particular system, machine, or equipment. These sensors capture data on the amount of vibration and transmit it to a system that can analyse and interpret the data. The primary purpose of a vibration sensor is to detect imbalances, misalignments, or other issues in machinery or equipment, enabling maintenance personnel to take corrective action before a breakdown occurs. By monitoring vibrations over time, vibration sensors can predict when a component will fail, allowing for planned maintenance instead of unexpected downtime. Vibration sensors are used in huge amount in industries, from manufacturing and construction to aerospace and transportation. These sensors can also be used to ensure safety in high-risk environments, such as

nuclear power plants or chemical processing facilities. In summary, vibration sensors are an essential tool for monitoring the health and safety of critical equipment, helping to prevent damage, downtime, and accidents.

15.2.12 Tracker

A tracking device refers to a mechanical or electronic device that enables an individual to remotely track the movement or location of an object or person. This device is capable of storing geographic data for future analysis and can also allow real-time monitoring of movement. The term “tracking device” encompasses a wide range of devices, including those that enable the storage of geographic data and those that allow the tracking of movement in real-time.

15.2.13 Battery

Battery is a crucial device that stores energy and then converts it into electrical energy by utilizing one or more electrochemical cells. Typically, batteries generate electricity through chemical reactions. There are various materials that can be used in batteries, but commonly used battery types include alkaline, lithium-ion, lithium-polymer, and nickel-metal hydride. These batteries can be connected in a series circuit or a parallel circuit, depending on the application.

There is a diverse range of batteries available in the market, and they are used in different devices. For instance, battery have many uses, they are used to start cars, while smaller ones can power hearing aids. Batteries play a vital role in everyday life, powering devices that we use daily, including smartphones, laptops, electric vehicles, and many more. With the growing demand for portable devices, there has been a significant increase in the production and use of batteries, and advancements in battery technology have led to improved performance, longer lifespan, and better safety standards.

15.3 About the Model

This model aims to create an intelligent smart shoe for individuals with visual impairments. The model is based on the philosophy of Hugh Herr, who stated that people are not “disabled” but that the built environment and technologies are flawed. The smart shoe is equipped with sensors that can detect obstacles in front of the person and provide warning signals in the form of vibrating sensations and beeping sounds.

This feature will help the visually impaired person to identify obstacles and avoid collisions. The shoe also includes a tracker that can monitor the person’s location. Additionally, the model incorporates a fire detection sensor that alerts the person if

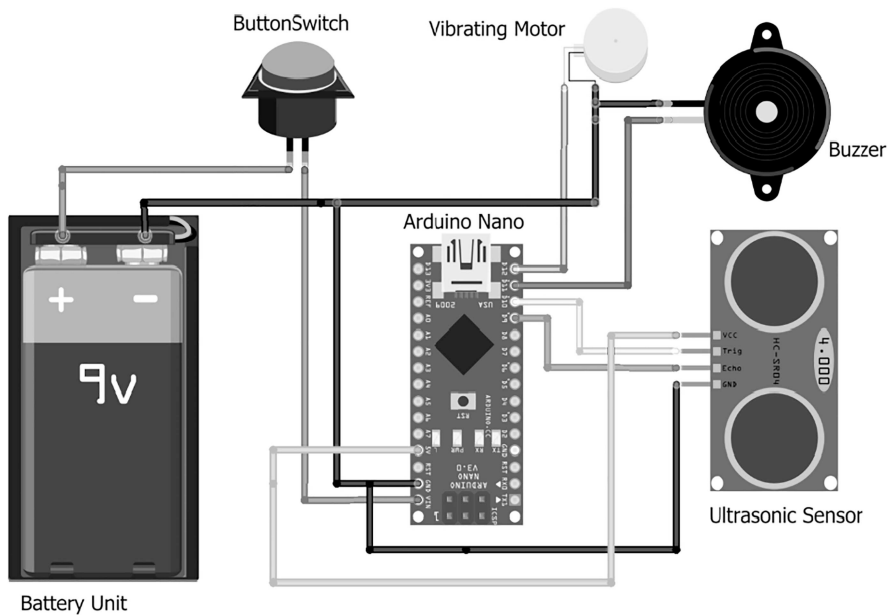


Figure 15.7 Schematics for ultrasonic sensor.

there is a fire in the vicinity. The integration of these technologies into the smart shoe provides a practical and innovative solution for individuals with visual impairments.

Schematics

To start assembling the components of our smart shoe model, we will first make connections between the Ultrasonic sensor and the Nano board. We will use Digital pins 10 and 9 to connect the Trigger and Echo pins, respectively. The VCC pin of the sensor will be connected to 5V, and the GND pin will be connected to the GND pin on the Nano board. After that, we will connect the Buzzer to the Nano board. The positive terminal of the Buzzer will be connected to Digital pin 11, while the negative terminal will be connected to the ground. Similarly, we will connect the Vibrating motor to the Nano board by connecting the positive terminal to Digital pin 12 and the negative terminal to the ground. To power up the model, we will connect the battery connector and switch module separately (Figure 15.7).

The button switch pin will be connected to the Vin pin of the Nano board, and the negative terminal of the battery will be connected to the GND pin of the Nano board. We will also integrate the Fire Detection sensor into the circuit. Furthermore, we will install a tracker in the shoe and connect it to the phone. Finally, we will assemble all the components together and fix them on the shoe (Figure 15.8).

DESIGN/PROTOTYPE

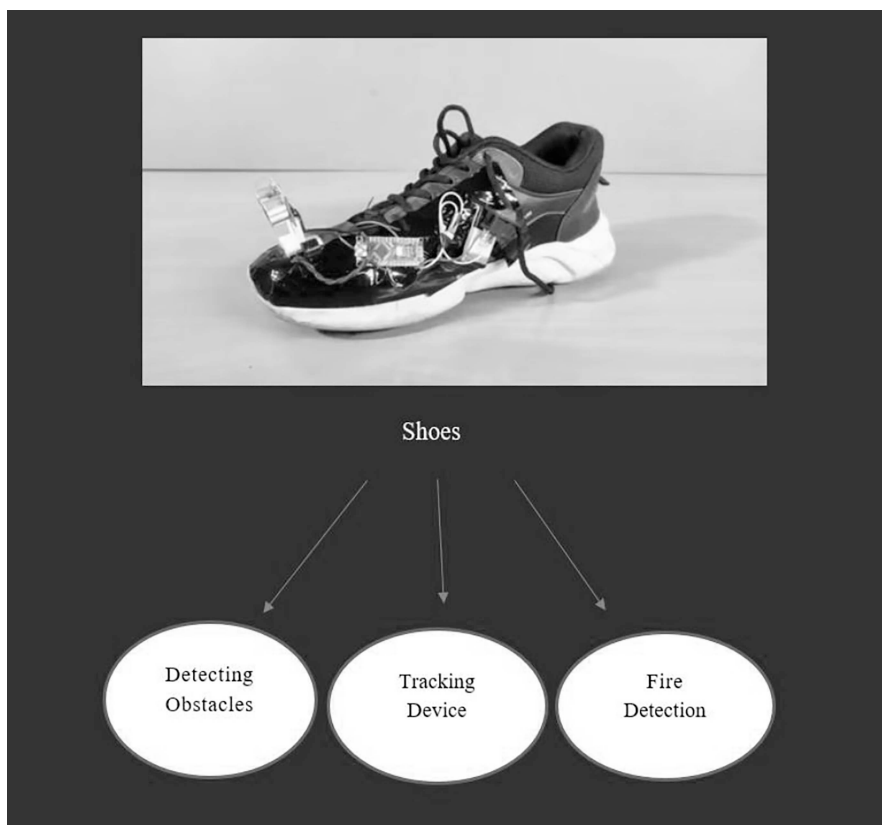


Figure 15.8 Proposed model.

15.4 Results and Analysis

With the help of this device, we are trying to solve some problems of blind people by making “Smart Shoe for Blinds”.

- **Detecting Obstacles and Warning – (Arduino and Ultrasonic).**
Many big challenges are faced by blind person, one of them is to find obstacles around them and get safe. So, with the help of shoes, we can help them to find obstacles in front of them and give them a warning by beeping sound or by vibration.
- **Fire Detection and Warning – (Fire Alarm).**
As blind people can't see and many of them are not able to make them safe from fire, and they die so to prevent there, life safe from fire, we are using fire alarm which will make them aware of fire around them by making some sound so that they can move to the safest place.

■ Tracking the location – (Tracker).

As blind people get confuse with the direction and move to other unknown places and are not able to find there, way or they are in some danger and did not reach home on time, then with the help of tracker, there family members can find their location easily and get them back. In this way, blind people will be safe.

15.5 Conclusion

With the help of smart devices and sensors, we can help humankind. The shoe with three devices: Ultrasonic sensor, a tracking device, and Fire Detector, will help a person in the following ways:

1. Making them aware of nearby obstacles while walking.
2. Providing information about the location of person (wearing the shoe).
3. Alerting them to the presence of fire or smoke nearby while walking.

Index

- Aadhaar enabled payment system in India, 127, 143
- AbdulWahhab, R. S., 232
- Academic outcomes, 80, 82, 90
- Access to banking services, 127, 129–131, 134
- Accuracy, 1, 15, 32, 69, 96, 111, 132, 155, 171, 181, 185, 189, 204, 215, 223
- Actuators, 16, 17, 25, 31, 46, 59, 62, 83, 91, 92, 190, 191, 203, 205
- Adaptation, 51, 71, 74, 86, 110, 135, 141
- Advanced Analytics, 64, 68, 69, 74, 128, 161, 201
- Affordability and accessibility of IoT devices and services, 135
- Agronomists, 95, 96, 99, 102
- Air pollution, 25, 26, 218, 219, 232
- Airspace, 99, 112
- Algorithms, 114, 116, 132, 147, 148, 150, 151, 160, 162, 167, 169
- Amazon server, 174, 181
- Ameer, S., 232
- Analytics, 4, 10, 20, 28, 29, 32, 34, 35, 39, 47, 50, 55, 62, 64, 68, 69, 73, 74, 76–79, 93, 109, 110, 115, 116, 123, 128, 150, 161, 166, 184–186, 188, 189–194, 198, 199, 201–203, 209–214
- Analytics of Big Data
 - biases, 55
 - challenges, 27, 46, 186
 - cloud computing, 31, 184, 193, 201
 - heterogeneity, 27, 46, 186
 - image processing, 184, 186–189
 - internet of things (IoT), 186
 - Internet of Things (IoT) Analytic, 186
 - real-time nature, 187
 - time and location, 187
 - varying quality, 187
- Android app, 119, 122, 123
- Application layer, 9, 11, 12, 19, 20, 52
- Applications, 31–34, 53–56, 60
- Arduino, 176–178, 219, 220, 226, 234
 - Nano, 234, 236, 239, 240, 245
 - Pin Functions, 238, 239
 - Special Pin Functions, 238
 - UNO, NANO, 234, 236
- Art, 3, 83, 156
- Associated technology, 47
- Atmospheric gas, 220, 221, 223
- Attacks, 21–25, 27, 147, 153, 154
- Authentication, 20, 21, 35, 40, 46, 47
- Authorized, 35, 48, 112, 207
- Autonomous learners, 83
- Ayele, T. W., 232
- Barberán, V., 232
- Beats per minute, 176
- Becnel, T., 232
- BGV, 161
- Big data analytics (BDA), 64, 79
- Billions, 8, 16, 21, 28
- Bizzotto, A., 232
- BLE-bluetooth low energy, 119
- Blind population, 234
- Blind/visually impaired individuals
 - navigation, 102, 235
- Blockchain, 40, 141, 150, 194, 210
- Block diagram, 160, 173
- Blood pressure, 26, 85, 163, 172
- Body temperature, 104, 172, 198, 208
- Bootloader, 223, 224, 226
- Brick-and-mortar, 61, 67, 73, 135
- Broker and message queue, 10
- Business layer, 19, 20, 51, 52
- Butterfield, A., 232
- Calculation, 219
- Cameras, 17, 24, 41, 91, 108

- Camprodon, G, 219, 232
- Carbon Monoxide, 218–221, 223, 229, 231
- Cardiac disease, 170
- Career readiness, 82
- Case studies
 - crop monitoring, 95, 97, 102, 105, 113, 196
 - livestock monitoring, 101, 104, 193, 198
 - pest management, 200, 208, 211
 - smart greenhouses, 209
 - smart irrigation system, 208, 211, 215
- Cloud, 4, 5, 31, 32–35
- Cloud API, 123
- Cloud application, 5
- Cloud-based architecture, 10
- Cloud platform, 5, 31, 200
- Cloud services, 10, 11, 47
- Coding, 83, 92
- Cognitive, 53, 83, 84, 164
- Collaborate, 82, 140, 206
- Communication, 5, 83–85, 87
- Communication system, 6
- Comparison, 124, 162, 180, 181
- Comprehensive, 57, 82, 83, 100
- Concerns, 46, 54, 65, 84
- Conclusion, 13, 28, 40, 56, 78
- Connectivity and communication
 - Bluetooth, 205
 - cellular networks, 205
 - low-power wide-area networks, 206
 - radio frequency identification, 205
 - Zigbee, 205
- Consumer protection, 134, 139, 140, 141
- Consumer rights and protection, 131
- Consumption, 140, 144
- Contextualized Recommendations, 69
- Control, 136, 147, 187, 194
- Control systems
 - livestock management, 192–195, 202, 204
 - precision farming, 95–98, 204, 206
 - smart irrigation, 104
- Conventional, 147, 150, 151
- Cost, 100, 129, 130, 135, 191
- Cost efficiency and scalability, 136
- Creativity, 56, 73, 82
- Credit and lending, 130, 131
- Cross-selling, 69
- Crucial, 83, 97, 112, 119, 141, 153
- Cultural and social barriers to adoption, 135
- Curve fitting, 220, 223
- Customer experience, 63, 72
- Customer lifetime value (CLV), 65, 71
- Cybersecurity, 113, 140
- Daneshmand, M, 232
- Data, 4–7, 9–13, 15, 19–22
- Data acquisition component, 6
- Data analysis, 25, 91, 130
- Database, 20, 30, 33, 34, 41, 152
- Data board, 221
- Data collection, 33, 199
- Data collection and analysis, 84, 85, 93, 127, 137, 194
- Data-driven insights, 167, 174, 176, 177, 179, 183
- Data privacy and security, 127, 135, 140, 143, 211
- Data processing component, 6
- Data security, 40–41, 46, 99, 153, 155, 158, 161, 207
- Data security issues, 83, 84
- Dataset, 151, 180, 219, 223, 228–231
- Decision support systems, 110, 202
- Deep learning, 132, 134, 185, 187, 202
- Deficits, 96
- Definitions
 - crop monitoring, 95, 97, 102, 105, 113, 196, 208
 - digital farming, 191
 - precision agriculture, 40, 102, 104
- DES, 147
- De Santis, A, 232
- Device compatibility, 44
- Device hardware, 5
- Devices, 6, 21, 26, 30–32, 34–40
- Device software, 5
- Devices required, 236
- Dhingra, S, 232
- Diagram, 165, 238
- Digital game, 84
- Digital identity and KYC, 140
- Digital literacy, 141
- Digital payments and mobile banking, 132
- Digital signage, 75, 76
- Ding, Y, 232
- Diseases, 97, 102, 103, 105, 106, 170
- Diván, M. J, 232
- Doctor, 165, 173
- Domains, 81, 82, 158
- Drones, 185, 191, 201, 204, 206
- Duan, N, 217, 232
- Early childhood education (ECE), 82, 83
- Ease, 73, 161, 162, 236
- eBay, 21
- Edge computing, 35, 39

- Educational robots, 83, 84, 92
- Elaboration, 151
- Electro Cardiogram (ECG), 172
- Electronic healthcare, 150
- Emotional, 63, 70, 83, 86
- Encryption, 113, 134, 146–148, 150, 151, 153–163
- Energy management, 26, 46
- Enhanced access and connectivity, 136
- Environment, 16, 17, 21, 23, 26, 27, 28
- Environmental monitoring, 26, 103
- Espinosa, F, 232
- Ethical, 55, 56, 63, 82–84, 86–90
- Ethical issues, 82–84, 86–89
- Event managers, 11
- Expression, 83

- Fertilization, 98, 111, 191, 195, 199, 200, 209, 212
- Financial education
 - inclusion, 126, 128, 132, 134, 135, 137
 - literacy, 82, 83, 88, 93
- Financial inclusion, 126
- Financial services, 126–130, 133, 134, 136–143
- Fine particulate molecules, 218
- Firdhous, M. F. M, 233
- Fire detection sensor, 234, 236, 242
 - function, 45, 51, 56, 74, 147, 177
 - overview, 1, 62, 63, 96
- Firmware, 35, 36, 113, 119, 166, 220, 221, 223, 224, 226
- Three-Layer and Five-Layer Architecture, 8
- Fog-Based Structure, 11
- Frameworks, 48, 55, 56, 97, 100, 113–115
- Fully homomorphic encryption (FHE), 127, 151, 158, 160, 161
- Future advancements, 53
- Future challenge, 47
- Future-Specific Applications and Examples of IoT, 48
- future spectrum, 43

- Gaillardon, P. E, 232
- Galassi, R, 232
- Gambi, E, 232
- Gandomi, A. H, 232
- Gases, 26, 59, 218, 219, 220, 223, 229
- Gateway layer, 10
- Gaussian Naïve Bayes Model, 178, 180
- General Data Protection Regulation (GDPR), 151
- Geometry, 83

- Glass, T, 232
- Goffin, P, 232
- González, Ó, 232
- GPRS (General Packet Radio Service), 171, 172, 173, 235, 236
 - network, 210, 212, 214, 215, 216, 217, 219
- GSM (Global System for Mobile Communications), 52, 173, 181, 235, 236, 247
- Guan, H, 232

- Hacked, 21, 28, 29
- Hacking, 27, 147, 150
- Ha, Q. P, 233
- Hardware, 6, 7, 11, 12, 14, 28, 44, 159, 164, 166, 175, 186, 187, 220, 232, 237
- Hazardous, 103, 107, 242
- Health, 2, 7, 9, 13, 23, 25, 26, 30, 33, 37, 38, 48, 51, 67, 81, 82, 85, 88, 96, 101, 102, 104, 105, 106, 116, 119, 210, 211, 218, 219, 232, 233, 234, 244
- Healthcare, 2, 7, 13, 25, 26, 48, 118, 123, 144, 146, 144, 148, 164, 167, 168, 170, 171, 172, 182, 183, 187
- Health data, 118, 146, 147, 148, 150, 152, 163, 164, 166, 209
- Health Insurance Portability and Accountability Act (HIPAA), 153, 164, 168
- Heart attack, 171, 174, 178, 179, 181, 182
- Heart health, 123, 124
- Heart rate, 85, 91, 104, 119, 120, 122, 124, 125, 163, 172, 198
- High prices, 83, 84, 127
- Historical, 105, 109, 110, 128, 202, 203, 204
- Holistic development, 81, 82, 88, 89, 92, 93
- Homomorphic encryption, 147, 150, 151, 159, 160, 161, 163, 165, 166, 167, 168, 169
- Horizons, 79, 81
- HTTP protocol, 123
- HTTPS, 148, 163
- Huang, J, 232
- Humidity, 26, 31, 85, 91, 92, 96, 104, 198, 200, 205, 209, 220, 221, 223, 229, 231
- Hyper-personalization, 67

- Identification, 26, 39, 57, 101, 105, 125, 134, 138, 140, 187, 188, 205, 214
- IFTTT, 5, 123, 124
- Illnesses, 96, 171
- Imagery, 40, 96, 98, 102, 111, 191, 200, 201
- Imagination, 83

- Immersive, 61, 67, 78, 81, 82, 216
- Immersive experiences, 67
- Industry, 3, 8, 17, 21, 30, 31, 38, 44, 48, 58, 55, 60–63, 67, 68, 74, 75, 78–80, 95–97, 101, 103, 112, 114, 117, 126, 131, 134, 140, 153, 156, 157, 172, 191, 210, 212
- Infestations, 96–98, 102, 105, 106, 111, 114, 115, 197, 209
- Innovative, 41, 49, 52, 54, 67, 81, 82, 138, 139, 142, 167, 182, 191, 234, 235, 245
- Insects, 97
- Instructional strategies, 81, 82, 88, 90–93
- Insurance and risk management, 130, 131
- Integration, 4, 6, 7, 12, 32, 40, 41, 50, 52–55, 63, 64, 77, 78, 81, 82, 95–101, 103, 105–117, 140, 141, 158, 164, 185, 186, 188, 189, 191, 194, 202, 206, 210, 211, 212, 235, 245
- Integrity, 21, 22, 24, 31, 33, 40, 53, 99, 113, 134, 140, 147, 148, 154, 155, 163, 164, 166, 185, 207, 210
- Intel Edison, 176, 177, 178
- Interactive, 62, 75, 76, 83, 84, 85, 161, 219
- Internet, 16–18, 21–23, 25–27, 29
- Internet of Things (IoT), 1, 2, 4, 6, 8, 10, 12, 14–16, 18, 20, 22, 24, 26, 28–30, 32, 34, 36, 38, 40, 42–46, 48, 50, 52, 54, 56–59, 62, 64, 66, 68, 70, 72, 74, 76, 78–82, 84, 86, 88, 90, 92, 94, 96, 98, 100–102, 104, 106, 108, 110, 112, 114, 116–120, 122–124, 126–128, 130, 132, 134, 136–138, 140, 142, 144, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 171, 172, 174, 176, 178, 180, 182, 184–186, 188–217, 220, 222, 224, 226, 228, 230, 232, 236, 238, 240, 242, 244, 246
 - applications, 7
 - architecture, 8, 50
 - hardware, 5
 - history, 1
 - introduction, 1
 - objectives, 3
 - plaything, 123
 - privacy, 12
 - security, 12
 - software, 3, 4, 5
 - spectrum, 44, 47
- Interoperability, 47, 49, 50, 99, 164, 166, 185, 210, 211, 212
 - standards, 180
- Interpretation, 140, 147, 151, 153, 166, 168, 188, 211, 244
- IoT-enabled financial inclusion, 126–129, 131, 133–143, 145
- IoT-enabled microinsurance, 139
- Islam, S. U, 232
- Jiménez, J. A, 232
- Ji, P, 232
- Karunaratne, P. M, 233
- Kelly, K, 232
- Key, 2, 3, 14, 20, 22, 31, 34, 35, 38, 39, 53, 57, 63, 64, 67, 75, 82, 96, 97, 108, 110, 114, 115, 129, 130, 132, 140, 147, 150–152, 154, 156, 158, 160, 163, 164–166, 177
- Key findings, 115, 152, 154, 156, 158
- K-Nearest Neighbor (KNN) algorithm, 132
- KNN model, 178, 179
- Kong, W, 232
- Lê, K, 232
- Level, 2, 5, 6, 13, 19, 35, 51, 52, 62, 74–78, 90, 92, 125, 130, 138, 157, 162, 163, 173, 176, 177, 181, 208, 209, 220, 221, 223, 228–231, 239
- Leveraging, 64, 65, 68, 79, 96, 105, 115, 129, 139, 140, 143, 193, 196, 199–204, 207, 209, 211, 216, 235
- Light, 31, 57, 104, 150, 176, 200, 209, 220, 221, 223, 229, 231
- Limitations, 21, 83, 88, 89, 92, 98, 101, 139, 152, 154, 156, 158, 217
- Linear regression, 178, 179, 220, 223, 228–231
- Literacy, 82, 83, 88, 93, 129, 130, 133, 135, 136, 140, 141, 143, 211
- Literature review, 82–84, 86–92, 100, 130, 148, 151, 167, 171, 217
- Liu, Z, 233
- Logged, 165, 224
- Logic, 20, 50, 84, 92
- LoRaWAN, 108, 215, 232
- Ma, C, 232
- Machine learning algorithm, 21, 35, 174, 178, 181, 194, 202, 215, 232
- Machine learning (ML), 53, 183
- Madda, R. B, 232
- Maple, C, 232
- Materials, 73, 87, 88, 93, 117, 151, 172, 187, 216, 244

- Matlab analytics cloud, 123
- MCU, 120
- Medical-cyber-physical systems (MCPs), 147
- Méndez, M. J., 232
- Methods, 3, 5, 44, 58, 74, 87, 91, 92, 99, 103, 107, 127, 132, 142, 148, 151, 153, 154, 160, 161, 164, 168, 181, 188, 193
- Metia, S., 233
- Microchips, 17, 21
- Microfinance, 133, 136, 138
 - risk management, 139
- Monitoring, 25–26, 192–200, 202–214, 216–221, 223, 225, 229, 231–233, 243, 244
- M-Pesa in Kenya, 143
- Mukherjee, S., 233
- Multispectral, 102, 105, 108, 111
- Music, 83

- NB-IoT, 46, 108
- Network, 1–3, 9–12, 14–24, 28, 31, 35, 36, 40, 41, 45–49, 51–58, 61, 62, 73, 82, 87, 92, 95, 96, 108, 118, 125, 129, 132, 134, 140, 142, 144, 150, 155, 156, 163, 167
- Network architecture, 28, 44
- Network layer, 2, 9, 12, 18, 20, 51, 185, 191
- NFC, 9, 20, 46, 120
- Nitrogen Dioxide, 218–223, 229, 231
- Noise, 35, 95, 91, 92, 100, 172, 187, 219–221, 223, 229, 231
- Noise sensor, 220, 221
- Numeracy, 83
- Nutrients, 98, 197, 212

- Objects, 8, 16–17, 31, 54, 61, 62, 92, 188, 235, 240
- Omni channel experiences, 62, 67
- OneM2M, 48, 50, 56, 58
- Operate, 16, 49, 107, 111, 114, 160, 176, 204, 207
- Operations, 40, 51, 53, 58, 61–63, 73, 74, 78, 85, 86, 93, 96, 99, 100, 107, 107, 110–116, 134, 147, 155, 160–163, 191, 192, 195, 203, 204, 206, 207, 210, 212
- Optimization, 62, 97, 98, 100, 115, 163, 164, 167, 189, 191, 192, 194, 203, 206, 212–214
- Oscillating system, 175
- Oxygen saturation, 172, 173

- Panebianco, J. E., 232
- Parental involvement, 83, 84
- Parr, B., 232
- Partially Homomorphic Encryption (PHE), 160, 161
- Particulate matter, 219, 232
- Patan, R., 232
- Patient, 15, 23, 48, 122–125, 146, 149, 150, 152–154, 156, 164–166, 171, 175, 182
- Patterns, 31, 37, 53, 69, 83, 84, 90, 92, 96, 98, 102, 104, 105, 109, 110, 114, 132, 187, 198, 199, 202, 205, 209, 210, 215
- Pedagogical, 83, 84, 86, 88, 90
- Pedagogical issues, 83, 84, 88, 90
- Perception layer, 8, 12, 17–20, 51, 191
- Pérez, M., 232
- Personalization of learning, 86, 87
- Personalized, 39, 49, 61–72, 78, 79, 81, 82, 85, 86, 88, 90, 92, 127, 134, 136, 141
- Personalized learning experiences, 81, 82, 85, 86, 88, 90, 92
- Phung, M. D., 233
- Physical, 6, 8, 9, 10, 16, 17, 20, 25, 27, 28, 30, 31, 51, 60–63, 67, 73, 81–83, 85, 87, 88, 92, 93, 120, 127, 139, 147, 151, 154, 157, 188, 178, 182, 185, 191, 205
- Physical layer, 8, 10, 17, 20, 51
- Physics, 83, 182, 189
- Playful, 83
- Policy effectiveness, 89
- Pollution, 26, 100, 103, 218, 219, 228, 229, 232
- Potgieter, J., 232
- Power management, 25, 101
- PPG data, 124
- Precision, 40, 95–98, 100–104, 106, 107, 111, 112, 115–117, 156, 191–194, 196, 197, 202–204, 206, 207, 211, 214
- Prediction, 57, 109, 166, 181, 183, 210, 212, 214, 223, 228, 230–233
- Predictive, 35, 38, 39, 47, 48, 62, 68, 77, 109, 116, 192, 194, 198, 199, 201, 202
- Prenatal, 146–148, 150, 164
- Preserving, 154, 155, 158, 160, 161, 163, 166, 168
- Prisma, 149
- Privacy, 31, 35–41, 47, 52, 146, 212
- Privacy and security concerns, 143
- Process, 31–25, 38–40, 184, 185
- Processing layer, 19, 20, 51, 52

- Process layer, 10, 20, 185
- Proposed model, 163, 246
- Protection, 12, 25, 27, 29, 36, 40, 53, 65, 102, 105, 107, 112, 113, 130, 131, 134, 140, 141, 151–153, 167, 198, 214
- Protocols, 3, 11, 23, 28, 29, 36, 40, 41, 56, 108, 147, 112, 115, 147, 148, 163, 189, 191, 207, 211
- Public-key, 160
- Public-private partnerships, 141
- Pulse sensor, 175
- Quality of life, 85, 86, 93, 138, 235
- Raspberry Pi3, 175, 176
- Real-time, 70, 73, 75–78, 81, 82, 87–92, 192–204
 - inventory management system, 76, 79
 - mobile healthcare, 172
- Recent years, 63, 147
- Regulatory frameworks, 140, 143
- Reliability, 22, 24, 47, 86, 87, 89, 93, 136, 155
- Research, 2, 3, 8, 9, 12–15, 17, 23, 39, 41, 42, 51, 57, 58, 65, 67, 79, 80, 82, 84, 86–90, 92, 93, 100, 101, 115, 116, 126–130, 132, 134, 141–144, 148, 150–154, 156–159, 169, 172, 185, 190, 212–215, 247
- Research impact, 89
- Research objective, 129, 152, 154, 156, 158
- Research quality, 89
- Revolutionizing, 60, 61, 104, 116, 169, 194
- Robust, 35, 40, 52, 56, 62, 65, 78, 113, 127, 134, 140, 147, 148, 163, 164, 175, 207, 211
- Safe, 112–115, 127, 130, 134, 136, 137, 139, 147, 164, 246, 247
- Sai, K. B. K., 233
- Santos, C., 232
- Savings and investments, 120, 131
- Sayahi, T., 232
- Scalability, 11, 27, 47, 53, 54, 83, 86, 87, 89, 93, 100, 107, 114, 116, 136, 154, 185, 194, 201, 210
- Scan, 24, 120
- Scheme, 6, 58, 154, 161, 167, 168
- Science, 57, 73, 78, 79, 81, 83, 95, 117, 144–146, 169, 181–184, 189, 190, 214–218, 233, 247
- Secure Sockets Layer (SSL), 23, 148, 163
- Security, 46, 47, 57, 150, 151, 153–156, 161–167, 207, 216, 217
- Senigagliesi, L., 232
- Sensitive, 12, 35, 55, 76, 113, 135, 140, 146, 149, 151, 161, 163, 164, 166, 207, 211
- Sensor board, 219–223
- Sensors, 2, 8, 9, 16, 17, 25–28, 30, 31, 40, 41, 47, 48, 50–52, 57, 59, 62, 68, 69, 73–77, 82, 83, 91, 92, 95–99, 101, 102, 104–108, 111–120, 122, 125, 127, 132, 133, 136, 138, 139, 170–176, 181–183, 185, 190–217, 219, 221, 223, 232–234, 239, 240, 243, 244, 247
 - crop health sensors, 194, 197
 - health monitoring sensors, 198, 208
 - nutrient level sensors, 194, 197
 - soil moisture sensors, 96, 194, 195, 208
 - soil pH sensors, 195, 196
 - soil temperature sensors, 196
 - weather sensors, 97, 194, 197, 198
- Sequencing, 83, 92
- Server, 11, 22, 50, 122, 123, 150, 155, 171, 172, 174, 181, 220, 223, 231
- Service layer, 11, 12, 50, 51, 185
- Shah, M. A., 232
- Shield, 151
- Shi, H., 232
- Simple linear regression model, 178
- Simulation, 84, 167
- Single Architecture, 17
- 6LoWPAN, 48, 49, 56, 57, 58
- Smári, V., 232
- Smart, 2, 7–9, 12, 13, 15, 17, 25–29, 31, 33, 44, 45, 48, 50, 52, 54, 55, 58, 62, 73–79, 85, 90–94, 100, 101, 104, 117–120, 122–125, 128, 132, 133, 135–138, 144, 148, 163, 166, 171, 172, 177, 184, 187–203, 205–221, 223–235, 237, 239, 241, 243–247
- Smart classrooms, 85, 92
- Smart devices, 73, 77, 119, 205, 205, 235, 247
- Smart grids for Pay-as-You-Go Solar Energy, 138
- Smart healthcare, 7, 13, 25, 125
- Smart IoT-based air quality monitoring system, 219, 221, 223, 225, 227, 229, 231, 233
- Smart retail environments (SREs), 73
- Smart shelves, 48, 75, 76
- Smart shoes, 234, 235, 237, 239, 241, 243, 245, 247

- Smart Watch, 33, 118–120, 123, 124
- SOA-based architecture, 11, 12, 14
- Social, 13, 14, 21, 29, 43, 65, 66, 74, 81, 83, 85, 91, 127, 129, 132, 135, 141–143, 167–170, 235, 236
- Solar panel, 220, 221
- Solid, 151, 152, 166
- Somewhat Homomorphic Encryption (SHE), 160
- Song, H, 232
- Spectrum, 32, 43–51, 53, 54–59, 148
- Spectrum allocation, 43–46
- Speed, 26, 75, 132, 159, 162, 171, 198, 241
- Standardization, 3, 46, 47, 50, 55, 99, 115, 140, 194, 211
- Standards and framework, 48
- STEM, 83, 84
- Stewardship, 107, 209
- Storage, 11, 20, 28, 31, 33, 34, 41, 77, 108, 112, 113, 149, 147, 148, 163–165, 178, 185, 201, 216, 244
- Sudantha, B. H, 233
- Sultana, H. P, 233
- Sun, W, 232
- Support Vector Machine (SVM), 178
- Surveillance, 100, 115, 164, 171, 183
- Sustainability, 54, 57, 58, 63, 73, 74, 80, 85, 86, 93, 104, 112, 115, 142, 144, 191, 194, 195, 197, 202, 209–213, 215, 217
- Systematic review, 83, 84, 94, 151, 167, 168
- Systems, 21, 25, 26, 34, 35, 37, 41, 47, 48, 50, 51, 53–59, 62, 77, 79, 92, 98–102, 106–111, 113–116, 127, 128, 130–134, 136, 138–140, 144, 145, 147, 148, 151, 154, 160, 161, 167, 168, 178, 188–196, 198, 199, 202–217, 235, 242, 243
- Teacher training, 84, 88
- Technical difficulties, 88
- Techniques, 91, 92, 97, 99, 108–110, 113, 116, 132, 142, 160, 163, 164, 166, 183, 185, 187, 188, 192–194, 199, 201, 202, 211, 214, 217, 232
- Technologies, 2, 3, 10, 14, 19, 27–29, 31, 32, 34, 41, 44–48, 50, 51, 53–57, 60, 63, 67, 73, 74, 77, 80, 81, 93, 94, 96, 97, 99–101, 106, 108, 113–116, 118, 123, 125, 127, 139, 141, 143, 45, 150, 153, 154, 158, 159, 167–169, 176, 182–184, 187, 188, 190, 191, 193, 194, 198–206, 210–214, 217, 232–236, 244, 245
- access control, 22, 207
- accessibility, 22, 24, 107, 135, 138, 210–212
- cellular networks, 48, 54, 194, 205, 206
- cloud computing, 11, 20, 27, 31, 33, 46, 132, 145, 150, 174, 183, 184, 190, 193, 201, 212, 214
- data analytics, 10, 28, 35, 39, 62, 64, 68, 73, 78, 79, 109, 110, 115, 116, 190–194, 201–203, 210, 212, 213
- encryption and authentication, 194, 207
- Wi-Fi, 206
- wireless communication, 205
- Temperature, 26, 31, 51, 52, 85, 91, 104, 111, 122, 152, 172, 173, 191, 194–196, 200, 205, 206, 208, 209, 220, 221, 223, 229, 231
- Temperini, G, 232
- Themes, 82, 83
- Things, 1, 2, 4, 6, 8, 10, 12, 14–16, 18, 20, 22, 24, 26, 28–30, 32, 34, 36, 38, 40, 42–46, 48, 50, 52, 54, 56–59, 62, 64, 66, 68, 70, 72, 74, 76, 78–82, 84, 86, 88, 90, 92, 94, 96, 98, 100–102, 104, 106, 108, 110, 112, 114, 116–120, 122–124, 126–128, 130, 132, 134, 136–138, 140, 142, 144, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 171, 172, 174, 176, 178, 180, 182, 184–186, 188–217, 220, 222, 224, 226, 228, 230, 232, 236, 238, 240, 242, 244, 246
- Threats, 15, 21, 22, 24, 36, 52, 56, 78, 79, 106, 113, 147, 166, 207
- Three-layer architecture, 8, 9, 17, 51
- Tian, B, 232
- Tingey, K, 232
- Transformation, 2, 32, 35, 52, 53, 61, 74, 185, 201
- Transport, 19, 20, 25, 51, 52, 161
- Transport layer, 9, 19, 20, 51
- Treatment, 105, 148, 163
- Trends
 - data privacy, 211
 - digital divide, 211
 - edge analytics, 210
 - emerging technologies, 210
 - interoperability and standardization, 211
 - regenerative practices, 211
 - security, 211

- Ultrasonic sensor, 234, 239–241, 245, 247
 - schematics, 245
 - waves, 239–242
- Unmanned Aerial Vehicles (UAVs), 95, 96, 98, 100, 101, 108, 117
- Unwanted, 151, 161
- Usability, 24, 31, 41, 138, 164, 166
- Values, 28, 35, 63, 71, 73, 119, 161, 193, 180, 223, 228, 231, 239
- Vector, 151, 178
- Vibration sensor, 236, 243
- Virtual, 2, 16, 53, 61, 215
- Visualization, 35, 37–41, 50, 96, 108, 109, 166, 189
- Wang, B, 232
- Wang, G, 233
- Wang, W, 232
- Waste, 38, 85, 89, 97, 98, 102, 204, 208, 209, 212, 215–217
- Wearable, 15, 25, 26, 45, 48, 62, 77, 82, 85, 91, 104, 119, 122, 125, 132, 137, 163, 171, 182, 183, 198, 208
- Wearable devices, 82, 85, 91, 125, 182, 198
- Wearables, 203
- Weather, 2, 26, 40, 51, 84, 96, 97, 99, 105, 109, 110, 138, 139, 192, 194, 197–199, 201–203, 206, 210, 214
- Well-being, 56, 81–83, 86–89, 91–93, 104, 134, 138, 139, 143, 148, 163, 198, 199, 204
- Whitaker, J, 232
- WHO (World Health Organization), 234
- Wi-Fi, 16, 19, 20, 45, 52, 108, 194, 205, 206
- WiFi
 - configuration, 226, 227
 - module, 221, 222, 224
- Wirelessly, 16, 104, 119, 171, 195, 197–200, 208
- Woo, S. S, 233
- Workflow, 165
- Wu, W, 232
- Xiang, W, 232
- Xiong, N. N, 232
- Xiong, X, 232
- Yang, G, 233
- Yang, Z, 232
- Yu, Y, 232
- Zhang, D, 233
- Zhao, L, 232, 233
- Zhao, S., 232
- Zigbee, 19, 21, 28, 46, 49, 50, 56, 58, 176, 205



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>